**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**
**CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS**
**FACULDADE DE DIREITO**

# REGULANDO O MODERADOR, MODERANDO O (QUE É) REGULADO:
## Considerações sobre vigilância e proteção de dados no PL das *Fake News*

**ALINE CRISTINE SANTANA**

**Rio de Janeiro**
**2021**

**ALINE CRISTINE SANTANA**

# REGULANDO O MODERADOR, MODERANDO O (QUE É) REGULADO:
## Considerações sobre vigilância e proteção de dados no PL das *Fake News*

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. José Roberto Franco Xavier.**

**Rio de Janeiro**
**2021**

CIP - Catalogação na Publicação

Santana, Aline Cristine
SS232r Regulando o moderador, moderando o (que é) regulado: considerações sobre vigilância e proteção de dados no PL das Fake News / Aline Cristine Santana. -- Rio de Janeiro, 2021.
102 f.

Orientador: José Roberto Franco Xavier.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Naciona de Direito, Bacharel em Direito, 2021.

1. Desinformação. 2. Fake News. 3. Proteção de dados. 4. Regulação. 5. Vigilância. I. Franco Xavier, José Roberto , orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

**ALINE CRISTINE SANTANA**

# REGULANDO O MODERADOR, MODERANDO O (QUE É) REGULADO:
## Considerações sobre vigilância e proteção de dados no PL das *Fake News*

Monografia de final de curso, elaborada no âmbito de graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. José Roberto Franco Xavier**.

Data da defesa: 26 / 02 / 2021.

Banca Examinadora:

_____
Prof. Dr. José Roberto Franco Xavier (orientador)

_____
Profª Dra. Karina Denari Gomes de Mattos (Membra da banca)

_____
Profª Me. Larissa Lagos de Souza Lemgruber (Membra da banca)

**Rio de janeiro**
**2021**

*"Se é certo que o desenvolvimento de tecnologias eficazes*
*nos permite viajar de um lugar para outro,*
*que as comodidades tornaram fácil a nossa movimentação pelo planeta,*
*também é certo que essas facilidades*
*são acompanhadas por uma perda de sentido dos nossos deslocamentos.*
*Sentimo-nos como se estivéssemos soltos num cosmos vazio de sentido*
*e desresponsabilizados de uma ética que possa ser compartilhada,*
*mas sentimos o peso dessa escolha sobre as nossas vidas [...]."*

(Ailton Krenac em "*Ideias para adiar o fim do mundo*")

## AGRADECIMENTOS

Esta monografia é a concretização de mais uma etapa de muitos desafios, desencantos, conquistas e paixões vividas ao longo de seis anos. Por meio dela, celebro os aprendizados e as experiências divididas com pessoas queridas que, de perto ou longe, caminharam comigo essa jornada, em especial:

**À minha família de sangue**, pai, mãe, Laís, minhas avós, minha tia Maria Victória (minha grande inspiração), minha dinda do coração, Margareth (*in memorian*), pessoas que me ensinaram a perseverar na luta, mas também na paz de espírito, trazendo sempre comigo um provérbio *Yorùbá* que diz "origem é destino";

**Ao Rafael**, meu grande amor e melhor amigo, que esteve comigo aprendendo as lições dessa surpreendente caminhada até aqui; dividindo sonhos e colecionando tropeços, mas ainda assim persistindo feliz, como bom companheiro que é;

**Ao meu orientador**, José Roberto Xavier, que na grandeza de sua sabedoria, paciência e sutileza soube me dar muito mais do que eu merecia; um grande mestre, que me ensinou que o melhor e mais eficiente "Código" é a observação;

**Aos meus amigos de faculdade**, João Carrara, Jaqueline Cardoso, Thaísa Oliveira, Luan Oliveira, Clarissa Mendes, Lucas Valle e Matheus Ceia, que também se tornaram amigos de vida, com quem divido as mais bonitas expectativas para um mundo melhor;

**Aos meus professores**, mestres e incansáveis defensores do Direito à serviço da justiça, da sociedade e da democracia; com os quais aprendi boas, e também controversas, táticas de batalhas;

**Aos meus chefes e colegas de estágio** que exploraram em mim o avesso do que eu imaginava que poderia ser; que me fizeram descobrir limites e vocações adormecidas;

**A todos** que, de algum modo, contribuíram não apenas para que eu chegasse até aqui, mas também para que eu revisasse as minhas ações em benefício do mundo afora.

A vocês, a minha gratidão é contínua!

## RESUMO

O presente trabalho aborda a discussão sobre o combate à desinformação e os riscos que a proposta regulatória do PL das "*Fake News*" (PL 2630/2020) pode oferecer aos direitos fundamentais. Nosso objetivo é entender quais direitos estão em jogo no projeto, tendo como recorte de análise a redação do artigo 10º, que trata do dever de registro e guarda, pelos provedores de serviço, dos dados referentes à cadeia de encaminhamento de mensagens em massa. Nossa hipótese é que, além de violar direitos fundamentais, o artigo pode validar uma política de "vigilância distribuída" (BRUNO, 2013), convencionando medidas de rastreabilidade irrestrita dos usuários. Por meio da abordagem teórica sobre desinformação (FALLIS, 2015; WARDLE&DERAKHSHAN, 2017), proteção de dados (RODOTÀ, 2008; DONEDA, 2019) e vigilância (ZUBOFF; 2015; LYON, 2018) e da análise de constitucionalidade do texto legislativo, observamos que o artigo 10 não representa um mecanismo oportuno ao que se propõe, mas reacende a questão sobre se ampliar o alcance da vigilância seria o melhor caminho para preservar a esfera-pública democrática. Sustentamos, por fim, que instrumentos regulatórios dessa importância devem ser pensados mediante amplo debate público qualificado, visando incentivar, coletivamente, uma cultura de educação midiática voltada para a segurança da informação e para a proteção dos dados pessoais.



**Palavras-chave:** Desinformação; *Fake News*; Proteção de dados pessoais; Regulação; Vigilância.

**ABSTRACT**

This investigation approaches the discussion about combat against disinformation and the risks the "*Fake News*" Bill (PL 2630/2020) could cause to fundamental rights. Our objective is to understand which rights are at stake in that bill. More strictly, we focus on its article 10, which specifies the obligations of the service providers to register and hold data from mass message fowarding chain. Our hipothesis is that, in addition to violating fundamenal rights, the article 10 can legitimate an "distributed surveillance" policy (BRUNO, 2013), validating unrestricted users tracking measures.Through a theoretical approach to disinformation (FALLIS, 2015; WARDLE&DERAKHSHAN, 2017), data protection (RODOTÀ, 2008; DONEDA, 2019) and surveillance (ZUBOFF; 2015; LYON, 2018) and a constitucional analysis of the legislative text, we observe the article 10 is an inadequate mechanism to accomplish its purpose. Actually, It rekindles the debate about the extension of surveillance as the better way to preserve the democratic publich sphere. Finally, we sustain that important regulatory instruments like this should be thought within a broad and qualified public debate, aiming to stimulate information security and personal data protection education.

**Key words**: Disinformation; Fake News; Data Protection; Regulation; Surveillance.

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ADI | Ação Direta de Inconstitucionalidade |
| ANPD | Autoridade Nacional de Proteção de Dados |
| Art. | Artigo |
| CRFB | Constituição Federal |
| IBGE | Instituto Brasileiro de Geografia e Estatística |
| LGPD | Lei Geral de Proteção de Dados |
| MCI | Marco Civil da Internet |
| STF | Supremo Tribunal Federal |
| TSE | Tribunal Superior Eleitoral |
| UE | União Europeia |

## LISTA DE ILUSTRAÇÕES

# SUMÁRIO

# INTRODUÇÃO

A desinformação surge, enquanto tema de interesse para esse trabalho, bem antes da pandemia que afligiu o ano de 2020, cenário que entendemos ser o ápice da crise democrática e institucional que nos levou à soma de 239 mil mortes[1] em razão da negligência de representantes do Estado apoiados, em boa medida, por cidadãos desinformados. Após as eleições de 2018 no Brasil, as consequências da desordem informacional provocada pela atuação de organizações criminosas na propagação de notícias falsas para fins eleitorais, foi o primeiro motivo para buscarmos entender que respostas o judiciário, ou mais propositivamente o Direito, tinha para esse problema.

Desde então, acompanhar a impunidade de atores políticos assumidamente envolvidos com esquemas de produção e difusão de *Fake News*[2]; o despreparo de autoridades legislativas para enfrentar o caso[3]; o uso das instituições para o aviltamento moral de adversários políticos[4]; a disputa econômica pela regulamentação do tema[5]; e, por fim, as lamentáveis consequências[6] para a vida de tantas pessoas, trouxe a indignação necessária à motivação de um projeto de pesquisa que resultou no estudo sobre as propostas regulatórias da desinformação no Brasil.

---

[1] Em 16 de fevereiro de 2021, somavam-se no Brasil 239.777 mil mortes em decorrência da infecção por Covid-19. Optamos por disponibilizar o link de um veículo noticioso, pois o site com informações oficiais do Governo Federal estava fora do ar desde a data de 14/02/2021. Disponível em https://g1.globo.com/bemestar/coronavirus/noticia/2021/02/15/casos-e-mortes-por-coronavirus-no-brasil-em-15-de-fevereiro-segundo-consorcio-de-veiculos-de-imprensa.ghtml. Acesso em 16 Fev 2021.

[2] O GLOBO. "**TSE arquiva duas ações que pediam cassação de Bolsonaro**". Publicada em 09 Fev 2021. Disponível em https://oglobo.globo.com/brasil/tse-arquiva-duas-acoes-que-pediam-cassacao-de-bolsonaro-1-24876328. Acesso em 16 Fev 2021.

[3] UOL. "**Nenhum país do mundo tem conclusões sobre *Fake News*, diz relatora da CPI das *Fake News* no Congresso**". Publicada em 30 Abr 2020. Disponível em https://noticias.uol.com.br/politica/ultimas-noticias/2020/04/30/nenhum-pais-do-mundo-tem-conclusoes-sobre-fake-news-diz-relatora-de-cpmi.htm. Acesso em 16 Fev 2021.

[4] Imprensa STF. "**Plenário conclui julgamento sobre validade do inquérito sobre *Fake News* e ataques aos membros do STF**". Publicada em 18 Jun 2020. Disponível em http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=445860&ori=1 . Acesso em 16 Fev 2021.

[5] FOLHA-PE. "**Plataformas se movimentam para desidratar projeto no Congresso que prevê punição por *Fake News***". Publicado em 29 Mai 2020. Disponível em https://www.folhape.com.br/politica/plataformas-se-movimentam-para-desidratar-projeto-no-congresso-que-pre/142203/. Acesso em 16 Fev 2021.

[6] Portal da UNICAMP. "**Como a desinformação tem atrapalhado nossa resposta à Covid-19?**". Publicado em . Disponível em https://www.blogs.unicamp.br/covid-19/como-a-desinformacao-tem-atrapalhado-nossa-resposta-a-covid-19/ . Acesso em 16 Fev 2021.

A partir disso, buscamos aprofundar o nosso conhecimento por meio de cursos[7], seminários[8], materiais produzidos por organizações civis[9] e por pesquisadores de referência no assunto[10], para melhor compreender quais implicações tornavam tão complexo o tratamento da desinformação pelo Direito. Neste percurso exploratório, observamos que a situação da quarentena domiciliar na pandemia aumentou o tempo de exposição das pessoas à internet e, por consequência, os níveis de desinformação e os perigos cibernéticos aos quais elas estariam expostas.

Logo, percebemos que a questão do tratamento de dados pessoais, em especial a controvérsia sobre o direcionamento de conteúdos de interesse público pelos algoritmos, também seria uma problemática atravessada pelo fenômeno da desinformação. Isso porque, na medida em que as plataformas de mídia extraem os dados de acesso e navegação, estudam o comportamento e redirecionam conteúdo e propaganda de acordo com o perfil de cada usuário, opera-se um ciclo automatizado de desinformação e desserviço à democracia.

O uso de dados pessoais para "personalizar" a experiência do usuário em determinadas plataformas impede que pessoas cercadas por redes de desinformação tenham contato com

---

[7] (i) IDP. Curso de "**Direito Digital**". (Online). Ministrado entre 30 Ago a 24 Set de 2020. Disponível em http://conteudos.online.idp.edu.br/direito-digital .
(ii) ITS. Minicurso "***Fake News* – impactos na liberdade de expressão e democracia**". (Online). Realizado em Jul de 2020. Disponível em https://itsrio.org/pt/cursos/fake-news/.

[8] (i) CGI.Br. "**11º Seminário de Proteção à privacidade e aos dados pessoais**". (Online). Realizado entre 17 a 20 Nov 2020. Disponível em https://seminarioprivacidade.cgi.br/ .
(ii) INTERNETLAB. **IV Congresso Internacional Direitos Fundamentais e Processo Penal na era digital**. Realizado entre 24 Ago e 04 Set de 2020. Disponível em https://congresso.internetlab.org.br/.
(iii) OAB-PR. Seminário "***Fake News* e Cidadania: combate à desinformação e eleições de 2020**". (Online). Realizado em 07 Jul 2020. Disponível em https://www.youtube.com/watch?v=LH7RL8CHzdE.
(iv) OAB-SP. Webinar " **Questões jurídicas das redes sociais**". (Online). Realizado entre 11 e 12 Ago 2020. Disponível em https://www.sympla.com.br/oab-sp-webinar---questoes-juridicas-das-redes-sociais__926703.
(iv) UFRJ. Evento: "**Pandemia e desinformação: contexto, estratégias e práticas**". (Online). Realizado em 17 Jun de 2020. Disponível em https://eventos.ufrj.br/evento/pandemia-e-desinformacao-contexto-estrategias-e-praticas/**.**

[9] Algumas organizações que serviram de fonte para o estudo sobre desinformação e proteção de dados foram: Agência Lupa; Abraji; Associação Brasileira de Jornalismo Investigativo (ABRAJI); Coalizão Direitos na Rede; Comissão de Proteção de Dados e Privacidade da OAB-RJ; Data Privacy Brasil; Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INCT.CC); Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec); Instituto de Tecnologia e Sociedade (ITS Rio); Instituto de Referência em Internet e Sociedade (IRIS); Internet Lab; Instituto New Law; Laboratório de Políticas Públicas e Internet (LAPIN); Legal Hackers; Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS, entre outros.

[10] Dentre os pesquisadores do direito, cujos trabalhos contribuíram para delimitar o tema desta pesquisa, cita-se: Bruno Bioni (Uerj/Lavits/ Data Privacy Br); Chiara de Teffé (IBMEC/UERJ); Esteia Aranha (OAB-RJ); Danilo Doneda (IDP); Laura Schertel Mendes (IDP); Luiza Brandão (IRIS); Nina da Hora; Nina Santos (UFBA); Rafael Zanatta (Data Privacy Br); Sérgio Amadeu (UFABC); entre muitos outros.

fontes de conhecimento mais plurais. Assim, quanto mais se consome desinformação, mais fontes de desinformação são sugeridas. Atrele-se a isso o fato de que, cada vez mais, as atividades cotidianas têm sido mediadas por dispositivos e serviços oferecidos pelas grandes empresas de tecnologia, que, por sinal, detêm mais ingerência sobre o quê as pessoas querem consumir.

Que caminhos, então, vislumbrar para a solução deste impasse, que parece nutrir um círculo vicioso? Para além disso, o que autoriza as empresas de tecnologia a decidirem, por meio de algoritmos, como será o ambiente informacional de cada pessoa? Quais direitos individuais estão sendo preteridos nessa dinâmica?

Para propor um debate sobre essas questões, este trabalho foi dividido em três capítulos. O primeiro traz uma abordagem essencialmente teórica sobre os temas que orientam a nossa hipótese, isto é, a de que a proposta de regulação em curso no Congresso lança mão de mecanismos de vigilância para conter o problema da desinformação, em detrimento dos direitos fundamentais da autodeterminação informativa e da proteção de dados.

O segundo capítulo, por sua vez, traz uma contextualização histórica e legislativa da regulamentação do tema no Brasil, enfatizando a discussão que dá pano de fundo ao problema no cenário digital: a dificuldade de se pautar um debate sério acerca dos modelos regulatórios para a responsabilização dos intermediários e os desafios para conciliar regulação x liberdade dos modelos de negócio.

Por fim, o terceiro capítulo traz uma análise dos mecanismos de combate à desinformação propostos no PL 2630/2020, mais especificamente da medida prevista no artigo 10, visando identificar quais direitos são tutelados ou violados pela redação do dispositivo e, a partir de uma análise constitucional de seus elementos, discutir se a medida representa oportuna para o combate à desinformação no contexto digital.

Em linhas gerais, a discussão oportunizada neste trabalho permitiu compreender que o enfretamento da desinformação passa pela necessidade de que a sociedade e as instituições estejam cientes de como funciona a economia informacional das redes e como seus agentes intermediários elaboram estratégias para capitalizar as informações sobre o comportamento, a

vida privada e o pensamento humano. Por isso, sustentamos a importância de se pensar políticas para a promoção da educação midiática e para a regulação da sistemática das tecnologias que alimentam o processo de desordem informacional, visando incentivar, coletivamente, uma cultura de segurança da informação e da proteção dos dados pessoais.

# 1. DESINFORMAÇÃO, VIGILÂNCIA E PROTEÇÃO DE DADOS

Enquanto caminhávamos para a conclusão deste trabalho, o maior vazamento de dados revelado na história do país foi anunciado: 223 milhões de informações pessoais, incluindo CPF, endereço residencial, salário, *score* de crédito, histórico de consumo em lojas virtuais e fotos de rosto estariam expostos em fóruns na internet aberta e na *dark web*. Quando a notícia eclodiu no mundo digital, um jovem empreendedor brasileiro de 19 anos resolveu apostar no seu site de checagem de dados, anunciando-o no *Twitter*. Não tardou para que a aparente solução viralizasse nas redes, até chegar aos jornais: "Veja se o seu CPF está entre os 223 milhões vazados nesta semana"[11].

O conteúdo das notícias dava conta de que a checagem no site "Fui Vazado" seria a melhor maneira para descobrir quais dados estariam expostos e, assim, se proteger. O procedimento de checagem era simples: consistia em informar o CPF e data de nascimento para acesso à suposta lista de dados vazados e, após, confirmar quais informações da lista (endereço residencial, telefone, e-mail eletrônico etc) pertenciam ao titular do CPF pesquisado. Nas primeiras 24 horas o site recebeu mais de 445 mil confirmações de dados.

Curioso notar que, apesar da total ausência de transparência quanto à finalidade da coleta e o destino dos dados confirmados, milhões de brasileiros entregaram suas informações pessoais, confirmando-as a um site desconhecido, de configuração visual duvidosa, e cujo procedimento foi endossado pela desordem informacional das redes. Somente após investigações conduzidas pela Autoridade Nacional de Proteção de Dados (ANPD), o STF determinou a retirada do site do ar, por entender que sua atividade, que já havia coletado informações de 700 mil pessoas, oferecia riscos à privacidade e se enquadraria na hipótese de comercialização de informações sigilosas[12].

---

[11] A matéria do site "TecMundo", publicada em 29/01/2021 e posteriormente republicada por portais de notícias como Uol, IG Notícias, Portal R7 e Veja, orientou os cidadãos a checarem no aplicativo "FuiVazado" se alguma de suas informações pessoais estaria pública. Disponível em https://www.tecmundo.com.br/seguranca/210173-veja-cpf-entre-223-milhoes-vazados-semana.htm. Acesso em 02 Fev 2021.

[12] OLHARDIGITAL. "**STF tira do ar site Fui Vazado, usado em consultas de vazamento de dados**". Notícia (online), publicada em 8 Fev 2021. Disponível em https://olhardigital.com.br/2021/02/08/seguranca/stf-tira-do-ar-fui-vazado-usado-consultas-vazamento-dados/. Acesso em 8 Fev 2021.

A situação revela o cúmulo da ironia de se buscar a proteção de dados expondo-se ao risco. Por outro lado, também revela como os caminhos da desinformação podem nos lançar a uma seara de controvérsias no mundo dos Direitos, que ao afirmar as nossas liberdades (como a liberdade para dispor sobre o ambiente informacional) relativiza algumas garantias (como assegurar a proteção dos dados).

É nesta seara que cidadãos hiperconectados, sobretudo as novas gerações, acompanharam as grandes mobilizações políticas dos últimos tempos, viram o crescimento e a derrocada de líderes e governos e testemunharam o crescimento de um ecossistema de informações para a produção de conhecimento. É também neste cenário que temos observado muita precipitação para combater o fenômeno das notícias falsas, o conteúdo fraudulento, e todas as variações da desinformação que conduzem a uma percepção equivocada sobre os fatos e a realidade.

Assim, visando entender as bases deste fenômeno e as complexidades para contê-lo, nas seções a seguir abordaremos as principais referências teóricas que têm relacionado a desinformação aos riscos para a democracia, tendo a vigilância e a proteção de dados pessoais como paradigmas de análise.

## 1.1 Desinformação

A desinformação é prática identificada na humanidade pelo menos desde o Império Bizantino, no século VI, quando, segundo historiadores (DARNTON, 2017)[13], Procópio teria produzido crônicas falaciosas para manchar a imagem do então imperador Justiniano . Na história recente, a palavra foi utilizada pela primeira vez no contexto da Guerra Fria, quando a União Soviética adotou mecanismos de produção e difusão de informações político-ideológicas para despistar estratégias de governo e facilitar sistemas de espionagem por meio de uma

[13] DARNTON, Robert. **A verdadeira história das notícias falsas: séculos antes das redes sociais, os boatos e as mentiras alimentavam pasquins e gazetas na Europa**. El País Brasil, publicado em 1 mai 2017. Disponível em https://brasil.elpais.com/brasil/2017/04/28/cultura/1493389536_863123.html. Acesso em 12 Jan 2021.

unidade específica do *Komitet Gosudarstvennoi Bezopasnosti* (KGB), especializada em desinformação (*dezinformatsiya*).

Mais tarde, em 1972, o *Chambers Twentieth Century Dictionary* de Londres incluiria a expressão "*misleading information*" (informação enganosa) no seu acervo de definições, para contextualizar os crimes de roubo de dados públicos que começavam a despertar a atenção de órgãos estatais. Alguns autores referem, ainda, que apesar de o termo "desinformação" nem sempre ter estado presente no vocabulário comum, fato é que a sua prática esteve atravessada por costumes corriqueiros, como a contação de causos, piadas e mesmo as parábolas, tendo se sofisticado com o desenvolvimento da imprensa escrita.

Volkoff (2004)[14] destaca que esse processo de sofisticação também acompanhou a inexorável relação entre meios de comunicação e formação da opinião pública, fazendo com que a desinformação se transformasse cada vez mais em um instrumento político. É bem verdade, porém, que o sentido político da palavra "desinformação", hoje, abarca o complexo cenário de produção e consumo de informação que deve ser entendido, em grande medida, como consequência do avanço das tecnologias.

Por outro lado, os fenômenos culturais emergentes das redes fazem com que também a desinformação use a política a seu favor: isto é, a política como motivação para que a desinformação continue existindo. E nessa dinâmica de dupla interferência comunicativa surgem desafios nocivos às democracias contemporâneas, que têm na informação a base para a expressão das liberdades, a formação do conhecimento e a participação cidadã.

Neste sentido, buscando compreender quais desafios a desinformação impõe à conjuntura democrática, nas próximas seções abordaremos os principais referenciais teóricos que se propõem a explicar seu conceito e a relevância do combate a esta prática na sociedade atual.

[14] VOLKOFF, Vladimir. **Pequena história da desinformação: do cavalo de Tróia à Internet**. Curitiba: Editora Vila do Príncipe, 2004, p. 32-33.

### 1.1.1 Referenciais teóricos para a construção de um conceito

Desde que a editora do famoso Dicionário Oxford (2016)[15] reconheceu o verbete “pós-verdade” (*post-truth*) como a palavra mais importante do ano, convencionou-se relacionar o conceito de pós-verdade, hiper verdade ou pós-fato com a ideia de notícias falsas, ou no seu cognato literal em inglês, “*Fake News*”. Não tardou para que o termo "*fake-news*" fosse rapidamente inserido no imaginário popular para designar qualquer tipo de informação imprecisa, boato ou mentira, desprendendo-se do contexto original do jornalismo.

Assim, quando se fala em "notícia-falsa" seria natural imaginar um conteúdo jornalístico que foi forjado ou dissimulado com o propósito de enganar – a exemplo do "*yellow press"* ("jornalismo amarelo", que no Brasil foi chamado de "jornalismo marrom"), prática que ficou conhecida no final do século XIX, quando jornais concorrentes inventavam mentiras para desbancar o conteúdo uns dos outros. Contudo, a popularização dos blogs e redes sociais permitiu que a apropriação do processo noticioso ─ apuração, produção e divulgação dos fatos ─ se desse cada vez mais por agentes não-profissionalizados, fazendo com que a ideia de "notícia" se desprendesse da exclusividade jornalística.

Esse movimento trouxe, inclusive, uma nova configuração para a autoridade do discurso jornalístico, seja porque as pessoas passaram a consumir mais informação nos meios não-jornalísticos (redes sociais, mídia independente e aplicativos de mensagens), seja porque o custo de se produzir e replicar notícia ficou mais acessível, permitindo que "qualquer pessoa" pudesse se tornar um *broadcaster*.

Assim, em meio ao contexto social da hiperinformação – isto é, a sobreposição de ambientes informacionais simultâneos, contínuos, onde a preocupação com a origem, a autoria e a ética perde espaço para a lógica da velocidade e da conveniência – a incidência das *Fake News* foi assumindo um papel muito maior na legitimação descritiva da realidade, tendo por base a relativização dos fatos em busca da satisfação truísta. Em artigo publicado em 2016, quando o termo pós-verdade começou a ser associado à dinâmica das *Fake News* nas Eleições

[15] BBC. “***'Post-truth' declared word of the year by Oxford Dictionaries***”. Notícia (Online) publicada em 16 Nov 2016. Disponível em https://www.bbc.com/news/uk-37995600. Acesso em 17 Jan 2021.

estadunidenses, a comunicóloga Ivana Bentes prenunciou o inevitável processo de "desinformação" que se formaria a partir dali:

> Saímos do domínio dos fatos para uma ensurdecedora guerra de slogans, certezas e dogmas. Um fundamentalismo comunicacional que prescinde de argumentação. Verossimilhança e evidência são a matéria prima da pós-verdade e do pós-fato. Sua enunciação repetida e viralizada por muitos, sua expressão em imagens e memes antecipam o que queremos ver acontecer. Sua simples difusão e circulação, a quantidade de cliques e visualizações são o que dão legitimidade ao conteúdo que é exposto. **A visibilidade máxima, o compartilhamento, o engajamento em comentários e cliques são a forma de legitimação do pós-fato e da pós-verdade. Algo que não necessariamente aconteceu, mas que a simples enunciação e circulação massiva produz um efeito de verdade** (BENTES, 2016, s.p, grifos nossos)[16].

Muito embora Bentes não tenha usado propriamente o termo "desinformação" para classificar as estratégias utilizadas naquele contexto eleitoral, sua descrição é oportuna para abordarmos algumas possibilidades de difusão e circulação da desinformação que foram reproduzidas em vários países, inclusive nas eleições brasileiras de 2018.

Os autores Wardle e Derakhshan (2017)[17] apontam que apesar de a expressão "*Fake News*" ter sido apropriada inicialmente para descrever estratégias de manipulação da opinião política, sua utilização generalizada acabou abrangendo a ideia de desinformação, dificultando a compreensão de seus usos distintos, motivações e reflexos para a comunicação social. Diante disso, os autores sugerem que as fake-news não devam ser confundidas com a desinformação porque implicaria na banalização dos arquétipos ritualísticos da comunicação, que são precedidos por intenções, valores e disputas de poder concretizados pela linguagem.

Isso significa que a desinformação não é apenas uma notícia inverídica, mas todo tipo de ação, ideia ou pensamento que, dentro do processo comunicativo – agente, mensagem, intérprete –, é manifestado propositalmente para enganar o interlocutor. Assim, ao deslocar o

---

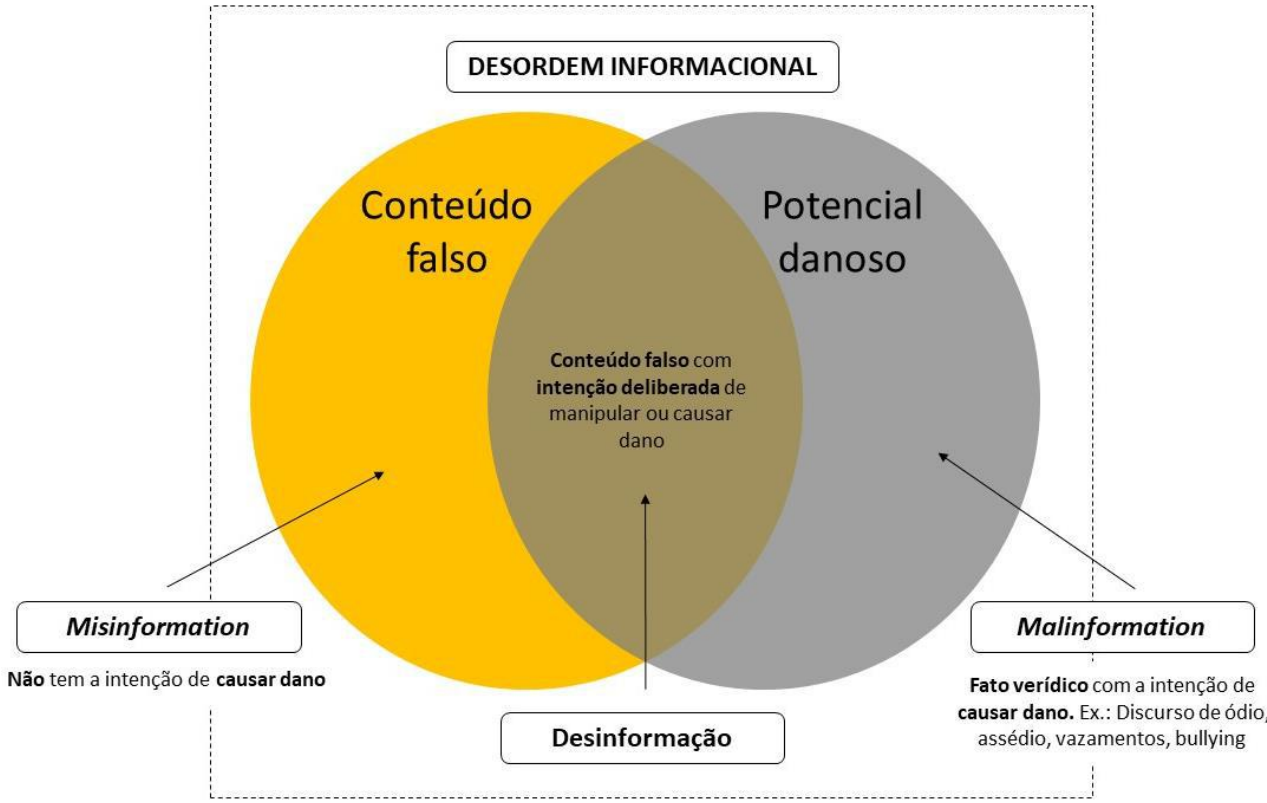
[16] BENTES, Ivana. **A memética e era da pós-verdade**. Artigo de opinião publicado em 31 Out 2016. Revista Cult, 2016, s.p. Disponível em https://revistacult.uol.com.br/home/a-memetica-e-a-era-da-pos-verdade/. Acesso em 18 Jan 2021.

[17] WARDLE, Claire; DERAKHSHAN, Hossein. *Information Disorder: Toward an interdiciplinary framewok for research and policy making*. **Council of Europe report (DGI)**, 2017, p. 20-26. Disponível em https://www.researchgate.net/publication/339031969_INFORMATION_DISORDER_Toward_an_interdisciplinary_framework_for_research_and_policy_making_Information_Disorder_Toward_an_interdisciplinary_framework_for_research_and_policymaking. Acesso em 27 Dez 2020.

foco do conteúdo para a ação, a abordagem de Wardle e Derakhshan traz uma importante contribuição para o desenvolvimento epistemológico de categorias de análise da desinformação, de acordo com a intenção e consciência dos atores que operam o processo comunicativo.

Para tanto, propõem três níveis de desinformação: desinformação (*dis-information*), que consiste em uma informação falsa, deliberadamente criada para prejudicar terceiros, grupos sociais, organizações ou instituições; *mis-information* (sem tradução), que consistente em uma informação inverídica, mas cujo intuito comunicativo não é enganar, prejudicar ou causar danos; *mal-information* (sem tradução), que consiste em uma informação baseada em fato verídico, porém dissimulada ou retirada de contexto para prejudicar terceiros, causar polêmica ou disseminar ideias contrárias ao fato narrado - neste último nível encontram-se o discurso de ódio, *revenge porn* e o *bullying*.

**Figura 1** - Níveis de desinformação e desordem informacional




Fonte: Elaboração da autora, 2021. Baseado em WARDLE E DERAKHSHAN, 2017, p. 20 (tradução nossa).

Além da classificação formulada por Wardle e Derakhshan, outros autores avançam no entendimento de que toda desinformação precede uma informação real, mas cuja interpretação dada pelo agente emissor, seja intencional ou não, é capaz de dissimular a representação da realidade. Para tanto, Fallis (2015)[18] destaca ser preciso antes fazer uma leitura filosófica do que seja a informação para então retirar o sentido concreto da desinformação.

Para o autor, a desinformação não pode ser lida como uma não-informação, mas como uma informação que não cumpriu o seu dever. Ele adiciona, ainda, duas classificações que complementam aquelas elaboradas por Wardle e Derakhshan, a saber: desinformação de efeito colateral (*side-effect disinformation*), isto é, a desinformação que não é desinformação na origem, mas se torna desinformação pela forma enviesada na qual é transmitida, a exemplo das informações em forma de sátira; e  informação adaptativa (*adaptive disinformation*), ou seja, aquela que pode ser dúbia, de duplo sentido, e cujo entendimento dependerá do contexto.

Há ainda quem adote classificações baseadas na credibilidade da fonte da informação, como no caso da "*junk information*" (informação lixo) adotadas por Marchal *et al* (2019)[19] para caracterizar as fontes inúteis de informações políticas que preencheram o repertório de notícias eleitorais propagadas no *Twitter*, durante as eleições parlamentares europeias em 2019.

De modo geral, observa-se que a mobilização de categorias de análise facilita a construção de um conceito possível para a desinformação, que, apesar de muitas elaborações, ainda não teve uma definição completa ou estruturada em conjunto com as áreas do conhecimento que são atravessadas pelos seus efeitos. Assim, na tentativa de empreender uma descrição multidisciplinar e viável à elaboração de políticas públicas para o assunto, o *High Level Expert Group on Fake News and Online Disinformation* (HLEG) da União Europeia propôs o seguinte entendimento:

> Informações falsas, imprecisas ou enganosas desenhadas, apresentadas e promovidas para intencionalmente causar dano público ou para obter ganhos econômicos. O risco

[18] FALLIS, Don. *What Is Disinformation?*. In: HEROLD, Ken (Coord.). *Exploring Philosophies of Information*. ***Library Trends***, Vol. 63, nº3. University of Illinois, 2015, p. 401-426. Disponível em https://www.ideals.illinois.edu/bitstream/handle/2142/89818/63.3.fallis.pdf?sequence=2. Acesso em 12 Jan 2021.

[19] MARCHAL, N., KOLLANYI, B., NEUDERT, L. M., & HOWARD, P. N. *Junk news during the EU parliamentary elections: Lessons from a seven-language study of Twitter and Facebook.* ***Online Supplement to Data Memo***, May 2019. Oxford Internet Institute, 2019, 1-12. Disponível em https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/EU-Parliamentary-Elections-Supplement.pdf. Acesso em 12 Jan 2021.

> ao dano público inclui ameaças ao processo democrático político e seus valores, o que pode ter como alvo específico diversos setores, como saúde, ciência, educação, economia e outros. Este processo é dirigido pela produção e promoção de desinformação para obter ganhos econômicos ou para atingir objetivos políticos ou ideológicos, mas pode ser exacerbado por como audiências e comunidades diferentes recebem, engajam e amplificam desinformação[20] (HLEG, 2018, p.3).

Em síntese, as *Fake News*, enquanto produto do tempo informacional do ciberespaço, são um fenômeno recente e podem ser compreendidas dentro de uma categoria maior, que é a desinformação. Logo, a *fake new* é uma desinformação que virou notícia, e sua divulgação, intencional ou não, contribui para a afirmação de uma pós-verdade e o consequente desarranjo informacional.

A pós-verdade, por sua vez, pode ser compreendida como um estado geral de circunstâncias, emoções e valores que levam à crença em determinada informação conforme a conveniência e relações identitárias entre agentes e intérpretes. Já a desordem informacional é o resultado causado por este processo de desinformação, operado pelas *Fake News* e tantos outros mecanismos, para literalmente desordenar a nossa capacidade de compreender a realidade. Daí porque muitos autores preferem o termo "desordem informacional" para se referir ao fenômeno, e desinformação para se referir às ações, levando em conta que as ações são identificadas pelas suas intenções, e o fenômeno é reconhecido pela soma da ação e do potencial danoso que ela gera na sociedade.

Por fim, cabe pontuar que, apesar de bastante elucidativas, tais definições se baseiam em estruturas argumentativas lineares, escapando-lhes as interferências subjetivas que os valores políticos, culturais e religiosos podem trazer para o entendimento do que seja "falso", "dissimulado", "impreciso" para cada pessoa. É, portanto, o risco que se assume ao operar categorias analíticas na pesquisa de fenômenos sociais.

---

[20] Na tradução livre do trecho original: "*False, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. The risk of harm includes threats to democratic political process and values, which can specifically target a variety of sectors, such as health, science, education, finance and more. It is driven by the production and promotion of disinformation for economic gains or for political or ideological goals but can be exacerbated by how different audiences and communities receive, engage, and amplify disinformation*". HLEG. "***A multi-dimensional approach to disinformation*".** Report of the independent High level Group on *Fake News* and online disinformation". Luxembourg: Publications Office of the European Union, 2018, p.3. Disponível em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271 . Acesso em 12 Jan 2021.

### 1.1.2 Desinformação enquanto problemática social em confronto com a democracia

Como visto na seção anterior, o alastramento das chamadas *Fake News* fez crescer a preocupação em torno das consequências da desinformação para a democracia, na medida em que passaram a ser usadas, de forma sistêmica, para a manipulação da opinião político-eleitoral. Por sua vez, o avanço das tecnologias e os arranjos informacionais das redes sociais fizeram com que o conteúdo jornalístico concorresse, no mesmo espaço, com o entretenimento e a visibilidade da vida privada, contribuindo para uma "poluição informacional" generalizada (WARDLE&DERAKHSHAN, 2017).

Tal circunstância permitiu que usuários com baixa instrução perdessem de vista a capacidade de discernir os critérios mais básicos de verificação de conteúdo e de credibilidade das fontes informativas. Do ponto de vista da segurança da informação, a ausência de discernimento sobre a legitimidade das fontes facilita que os usuários se exponham aos riscos de crimes cibernéticos mais evidentes, como furto de dados, golpes financeiros, assédio sexual, entre outros. Além disso, propicia um cenário confortável para a redução de debates públicos à memética, permitindo que o exercício da liberdade de expressão seja levado até o limite do desrespeito à coletividade.

É neste contexto que a fetichização dos discursos de ódio e ataques à ordem democrática e social ganha força, apoiada, sobretudo, na ideia de que a Internet é um espaço livre para a manifestação de qualquer pensamento e onde a desinformação é utilizada para validar pontos de vista pré-existentes, dissimulando ou descontextualizando fatos concretos (WALDMAN, 2017)[21]. Atrelado a esse aspecto, os sistemas algoritmos das redes impulsionam conteúdos de proveniência duvidosa, baseados no perfilamento do consumo cultural de cada pessoa, lançando os usuários – desde os menos esclarecidos até os mais instruídos – a fluxos informacionais cada vez mais automatizados e de repertórios monotemáticos.

[21] WALDMAN, Ari Ezra. *The Marketplace of Fake News.* Vol. 20. **University of Pennsylvania Journal of Constitutional Law**, 2017, p. 845-870. Disponível em https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1661&context=jcl. Acesso em 12 Jan 2021.

Assim, esses usuários têm limitado seu espectro de realidade a um cenário mais conformado com seus interesses individuais, reduzindo, portanto, seus esforços intelectuais de selecionar, checar e confrontar a informação. Trata-se, portanto, de uma dinâmica que, modulada pela pré-ordenação tecnológica, corrói um dos pressupostos mais fundamentais para o exercício da cidadania: a liberdade de escolha.

Tal sistemática é visivelmente preocupante, pois ao mesmo tempo em que abre espaços para inflar discursos extremistas e a polarização de pensamentos, a enunciação e circulação automatizada de desinformação produz "um efeito de verdade", como bem disse Bentes (2016), que aniquila a capacidade dos discursos científico e jornalístico de reerguer sua credibilidade no contexto da comunicação de massas. Logo, o que temos testemunhado com a proliferação desenfreada da desinformação é um colapso para as vias de sociabilidade humana, que, em 2018, foi definido pela Organização dos Estados Americanos (OEA) como algo "sem precedentes na história recente da América Latina"[22].

Como, então, pensar a subsistência dos modelos democráticos baseados no acesso à informação e na liberdade de expressão, se a hiperexposição das pessoas aos ambientes informacionais não as tem conduzido ao melhor exercício da cidadania? E como pensar o papel das empresas de tecnologias na modulação dos arranjos (e desarranjos) informacionais que as cercam? Neste sentido, considerando o processamento massivo de produção e consumo de informações na sociedade contemporânea a partir, principalmente, dos usos da Internet, abordaremos a seguir dois pontos que nos parecem centrais para refletir essas questões: o monitoramento de dados para a modulação de comportamentos (vigilância) e a proteção dos dados pessoais.

## 1.2 Vigilância

[22] EBC. "**Para OEA, difusão de notícias falsas no Brasil 'não tem precedentes'**". Notícia (online) publicada em 25 Out 2018. Disponível em https://agenciabrasil.ebc.com.br/politica/noticia/2018-10/para-oea-difusao-de-noticias-falsas-no-brasil-nao-tem-precedentes. Acesso em 18 Jan 2021.

Dificilmente poderíamos abordar os fenômenos tão próprios do mundo hiperconectado sem observar os efeitos que a cultura das redes tem produzido na política, na cultura, nas organizações sociais e nas subjetividades humanas. Como resultado disso, a vigilância, assim como a desinformação, teve seu curso radicalmente alterado pela organização e estrutura das redes, embora não seja prática inédita na história da humanidade.

É possível que a vigilância, enquanto instrumento de poder, tenha surgido ainda no século XVIII e atingido seu auge no século XX, com a decadência das chamadas "sociedades disciplinares", quando então foi profundamente incorporada às "sociedades de controle" (DELEUZE, 1992)[23]. Essa transição, marcada pelo esvaziamento de sentido da rigidez e do confinamento dos corpos físicos, deu lugar a modelos disciplinares cada vez mais abertos, flexíveis e contínuos (*idem*).

Com a emergência de um novo tempo social, a que muitos autores atribuem ao desenvolvimento e popularização das tecnologias de comunicação e informação (TICs), a vigilância do poder estatal já não representa a única via de controle sobre o comportamento humano, mas também há o domínio interiorizado na presença, quase absoluta, das tecnologias na vida das pessoas.

Esse novo cenário de aproximação dos aparatos de vigilância com as esferas da vida cotidiana produz novas subjetividades – humanas e tecnológicas – que estão em constante manutenção do funcionamento do sistema. Isto é, nas palavras de Deleuze, "vivemos um momento histórico no qual existem, simultaneamente, características da sociedade disciplinar em decadência e da sociedade de controle em expansão" (1992, p. 220).

Assim, objetivando entender como este modelo de controle se insere no contexto da "sociedade da informação", discutiremos, nas próximas seções, a que se deve a cultura de vigilância mediada por tecnologias de comunicação e como isso se traduz na expansão de um poder irrestrito, que atravessa a constituição dos sujeitos no universo digital e influi sobre mentes e corpos humanos.

[23] DELEUZE, Gilles. **Conversações**. Rio de Janeiro: Editora 34, 1992, p. 220-227.

### 1.2.1 A cultura da vigilância na sociedade da informação

O cenário que antecede a profunda conexão entre as mudanças político-culturais e os avanços tecnológicos promovidos pelo advento da Internet é marcado pela influência dos meios de comunicação de massa na produção e distribuição de produtos simbólicos, que se propunham a representar a realidade. A partir da década de 50, em meio à evidente aceleração das economias mundiais rumo ao posterior processo de globalização, o conceito de "Sociedade Global" começou a ser mobilizado por uma série de pensadores, dentre os quais cita-se Alain Touraine, Daniel Bell e Marshall Mcluhan, para explicar a comutação de fenômenos culturais, identitários, políticos e econômicos capazes de atravessar as fronteiras estabelecidas pela limitação geográfica e estatal.

Naquele contexto, tais autores identificavam os meios de comunicação de massa, sobretudo a televisão, como importante instrumento de poder para difundir uma mensagem, em quantidade e apelo cognitivo infinitamente mais eficazes do que os meios formais da época (rádio e canais impressos). Por seu turno, rapidamente a televisão foi considerada um dos principais instrumentos de expansão do capitalismo no século XX.

Mais tarde, com o desenvolvimento da informática e a consequente possibilidade de comunicação eletrônica por redes interligadas de sinais, o computador traz a possibilidade de concentrar várias funções comunicacionais para os usuários e minimizar os custos da produção e distribuição da informação pelos *mass media*. Inevitavelmente, tal característica leva à expansão, reestruturação e flexibilização do capitalismo pós-industrial rumo a um novo paradigma central na organização da sociedade global: a informação como elemento-chave para designar os fluxos produtivos.

Mas, enquanto a rapidez e eficiência dos avanços tecnológicos ditavam as regras econômicas e políticas, sobretudo nos países industrializados, aos países menos desenvolvidas restou o desejo de informatização que não acompanhou a desenvoltura estrutural dos países ricos, embora tenha-lhes cedido a irresistível influência da cultura das redes que começava a emergir. Observando esse movimento promissor e também ambíguo, o sociólogo Manuel

Castells (1999)[24] propôs entender os reflexos culturais, políticos e econômicos dessa nova ordem informacional, que chamou de "Sociedade em Rede", a partir da sua relação com o poder estatal.

Conforme sugere, a Sociedade da Informação pode ser entendida na "morfologia social" das Redes, que são compostas por atores de processos produtivos, dentre os quais situam-se os Estado, os sujeitos e os impérios de mídias, que utilizam as tecnologias de informação e comunicação para produzirem experiência, poder e cultura em escala mundial.

O autor salienta que, a partir dos anos 2000, a penetrabilidade e reversibilidade da informação enquanto matéria-prima, atreladas ao predomínio do computador sobre os outros meios e à crescente convergência com outros dispositivos – como mais tarde ocorreu com os celulares, a televisão e os automóveis – deram condições para que todo fluxo de ações dentro do espaço-temporal da Internet pudesse ser capilarizado e ao mesmo tempo integrado às "fontes cruciais de dominação e transformação de nossa sociedade" (CASTELLS, 1999, p. 565).

Castells avança para uma compreensão política das novas tecnologias, e por consequência das Redes, que está relacionada a sua instrumentalidade no processo de transformação do poder estatal, que se diferencia das táticas de governo baseadas no "poder soberano", conforme descritas por Michel Foucault. No poder soberano, é o Estado quem define a ordem e o limite das coisas; o que é de interesse público e de interesse privado; a disposição sobre a vida, já que a ele é reservado o poder de matar.

O poder exercido na Sociedade da Informação é diferente. A própria concepção de atuação do Estado não é una ou absoluta. Ela passa, precisamente, pela ideia de um macro-organismo constituído por uma pluralidade de atores menores e de conexões entre eles. São tempos que também denotam, na estrutura do poder governamental, a substituição gradual da coerção e da imperatividade pelo *soft power* da influência pacífica.

Mais do que dissimular a força e os esforços brutais do Estado, as relações de poder que atravessam os indivíduos pela ingerência das tecnologias são estabelecidas por um *biopoder*

[24] CASTELLS, Manuel. **A sociedade em rede. A era da informação: economia, sociedade e cultura**. Vol. 1. 2ª Edição. São Paulo: Paz e Terra, 1999, p. 565.

que instala nas microrrelações do cotidiano, e que intensificam e disciplinam os modos de viver mais do que limitá-los ou destruí-los.

> [...] A nova tecnologia que se instala se dirige à multiplicidade dos homens, não na medida em que eles se resumem em corpos, mas na medida em que ela forma, ao contrário, uma massa global, afetada por processos de conjunto que são próprios da vida, que são processos como o nascimento, a morte, a produção, a doença, etc. Logo, depois de uma primeira tomada de poder sobre o corpo que se fez consoante o modo da individualização, temos uma segunda tomada de poder que, por sua vez, não é individualizante mas que é massificante [... ] (FOUCAULT, 2002, p. 289)[25].

Esse é o ponto que sobrepõe o poder soberano de "fazer morrer e deixar viver" e passa a impulsionar a vida em todo o seu desenrolar, num movimento de constância no qual a vida é o que escapa; é o limite. Tudo o que está entre o viver e o morrer pode ser disciplinado pelo *biopoder*.

Com efeito, num dos mais importantes estudos sobre a evolução da sociedade disciplinar pela ótica dos sistemas punitivos, Foucault (2014)[26] observou que quando o poder estatal encontra o binômio tecnologia e visibilidade para operacionalizar seu modelo de disciplina, a lógica do controle já não se baseia no suplício, no espetáculo do sofrimento, mas no "estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder" (2014, p. 195).

Ao discorrer sobre as prisões modernas que operavam no modelo panóptico antes descrito por Bentham[27], onde a centralidade da torre de vigilância era visível por todos e ao mesmo tempo observava a todos, Foucault propôs que o poder disciplinar materializado nas prisões era uma espécie de "laboratório permanente", cuja eficácia e capacidade de penetração no comportamento das mentes desviantes poderiam ser replicadas em qualquer esfera da vida. Isso porque, a exemplo de como funcionava nas prisões, uma vez centralizada permanentemente à vista dos prisioneiros, porém sem que estes pudessem identificar quem os vigiava ou se os vigiava, a arquitetura panóptica induzia um comportamento automático baseado na dúvida constante de estar sendo vigiado e no medo da repressão.

---

[25] FOUCAULT, Michel. **Em defesa da sociedade**. Tradução: Maria Ermantina Galvão. São Paulo: Martins Fontes, 2002, p. 289.

[26] _____. **Vigiar e punir: nascimento da prisão**. Tradução: Raquel Ramalhete. 42ª Edição. Petrópolis: Editora Vozes, 2014, p. 194-202.

[27] Em referência à obra clássica do filósofo Jeremy Bentham. In: BENTHAM, J. **O panóptico**. Belo Horizonte: Autêntica Editora, 2008.

A avaliação de Foucault, todavia, tende ao reducionismo de um mundo marcado pela padronização dos espaços de controle, tais como os ambientes de trabalho, os reformatórios, as escolas etc, pouco avançando sobre as possibilidades de cooptação do comportamento fora desses espaços. A esse respeito, muitos estudos contemporâneos têm retomado as bases do modelo disciplinar-punitivo para compreender as práticas de vigilância no contexto atual.

Autores como David Lyon (2013)[28], Fernanda Bruno (2013)[29], Shoshana Zuboff (2015)[30] e outros apontam que, na sociedade da informação, as redes podem ser comparadas à torre de vigilância, porém administradas por agentes heterogêneos que se colocam não mais como delatores do comportamento desviante, mas como sujeitos que também fazem parte do "ambiente vigiado". Até porque, também na sociedade da informação há a expectativa da obediência, entretanto vem marcada por um discurso ameno, planejado para que haja pouca ou nenhuma resistência por parte dos "vigiados".

Ao passo que na lógica das sociedades disciplinares há a expectativa de que os comportamentos sejam previsíveis ou estáveis, na sociedade da informação essa expectativa encontra óbice nas possibilidades de autorreferência mediada, ou como sugere Castells (1999)[31] uma "autocomunicação", que passa pela construção autônoma de imaginários ideais para se espelhar – inspirando comportamentos variados, inimagináveis.

À primeira vista, o cenário da comunicação de massa *pós-broadcast* – isto é, um modelo de "distribuição sem precedentes de conteúdos, sem limitação de tempo e espaço e modos de acesso a um conjunto de plataformas, telas e produtos"[32] – transmite a ideia de que a estrutura das redes confere maior autonomia às escolhas dos usuários e, por isso mesmo, dificulta as estratégias de vigilância. Todavia, a capilaridade do uso de plataformas e dispositivos de mídia

---

[28] BAUMAN, Z.; LYON, D. ***Liquid surveillance: a conversation***. Cambridge: Polity Press, 2013.
[29] BRUNO, Fernanda. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade.** Porto Alegre, Sulina, 2013.
[30] ZUBOFF, Shoshana. *Big Other: surveillance capitalism and the prospects of an information civilization*. **Journal of Information Technology**. V. 30, nº1. US: Sage Publishing, 2015. Disponível em https://journals.sagepub.com/doi/10.1057/jit.2015.5. Acesso em 18 Dez 2020.
[31] Op. Cit. CASTELLS, 1999.
[32] BUONANNO, Milly. Uma eulogia (prematura) do broadcast: o sentido do fim da televisão. **Revista Matrizes** (USP). v. 9, nº 1, jan-jun de 2015. São Paulo: USP, 2015, p. 67-86. Disponível em https://core.ac.uk/download/pdf/268325468.pdf. Acesso em 22 Jan 2021.

amplia as possibilidades de registro sobre o comportamento humano, assim como estende aos intermediários privados, quais sejam, as empresas de tecnologia e de mídia, o poder de determinar as regras do jogo.

Atrele-se a isso o fato de que a era da autocomunicação de massa altera sobremaneira a economia da visibilidade sobre o comportamento humano, que desde as experiências dos programas televisivos de *reality show* vem sinalizando uma mudança de interesse nos conteúdos agendados para a autenticidade do cotidiano[33]. Nos *reality shows*, mesmo sabendo-se que o cotidiano midiatizado é, por assim dizer, "falso", a visibilidade sobre o que acontece no hipotético espaço privado dá a chance de qualquer cidadão comum verificar se aquele cotidiano é igual ao seu. Há um jogo de reconhecimento e de poder no imaginário da vida privada midiatizada, que ao mesmo tempo permite o sujeito-observador se reconhecer naquele simulacro e também julgar, ou até mesmo punir, os comportamentos dos sujeitos-observados conforme as regras do jogo.

Finalmente, há de se considerar que as mudanças de configuração desse novo imaginário influem sobre as táticas de conformidade operadas pelos indivíduos, que passam a ser observantes-observados numa relação de meta-vigilância cotidiana. Tenhamos como exemplo a tendência de expor a vida privada na Internet, que desde a popularização dos blogs e sites de redes sociais no início dos anos 2000, parece ter "ligado a chave" da cultura do "ser-parecer-ser" digital. Isto é, quando sei que estou sendo vigiado, ajo de determinado modo, e justamente por vivenciar [e, em alguns casos, almejar] essa vigilância, eu exponho as minhas maneiras de ser para parecer ser quem eu quero.

É neste sentido que David Lyon (2018) sinaliza a necessidade de entender a vigilância na sociedade da informação como uma "Cultura" que se relaciona com as maneiras de ser e de viver, isto é, algo que faz parte do cotidiano, dos valores, das escolhas pessoais, numa simbiose de sentidos e práticas. Ele acrescenta:

---

[33] Ver referência sobre a exposição do cotidiano no cenário da comunicação de massa em BALL, Kirstie.. *Exposure: exploring the subject of surveillance*. **Information, Communication and Society**. V. 12, nº 5. UK: Routledge, 2009, p. 639-657. Disponível em https://www.tandfonline.com/doi/full/10.1080/13691180802270386. Acesso em 22 Jan 2021.

> [...] Daí meu uso da palavra **Cultura**. **Não é mais apenas algo externo que se impõe em nossa vida. É algo que os cidadãos comuns aceitam – deliberada e conscientemente ou não –, com que negociam, a que resistem, com que se envolvem e, de maneiras novas, até iniciam e desejam**. O que antes era um aspecto institucional da modernidade ou um modo tecnologicamente aperfeiçoado de disciplina ou controle social hoje está internalizado e constitui parte de reflexões diárias sobre como são as coisas e do repertório de práticas cotidianas. (LYON, D., 2018, p. 152-153, grifos nossos)[34].

A passagem de Lyon embasa o conceito de "pós-panoptismo" que muitos estudos contemporâneos têm defendido, no sentido de que a vigilância, enquanto prática produzida e estruturada por tecnologias, está arrefecida com a lógica benthamiana de "ver e ser visto" e já não se sustenta apenas nas mãos do observador estatal. A lógica da vigilância na sociedade da informação está sedimentada na onipresença das tecnologias, mas não apenas em torno da consciência de estar sendo vigiado – essa, talvez, já "naturalizada" e às vezes até ausente de senso crítico – e sim na estratégia algorítmica que dissimula as causas e os efeitos da ação humana.

Ou seja, na medida em que se ampliam as possibilidades de vigilância – embora não necessariamente esteja mais visível – se torna mais difícil para o sujeito vigiado ponderar as consequências sobre suas ações e para discernir sobre o quê, precisamente, incide o controle. Não significa apenas dizer que a vigilância "se esconde", enquanto elemento invisível nas tecnologias, mas compreender que existem processos pré-designados, que estimulam a influência irrestrita dessas tecnologias nos modos de ser e viver.

Há algo de misterioso e ambíguo no funcionamento da vigilância pós-panóptica, que se distancia do poder exercido sobre a conformidade de estar sendo vigiado, mas ao mesmo tempo cria uma falsa impressão de autonomia sobre essa conformidade. A conformidade do modelo panóptico induzia determinado comportamento pelo medo da sanção consequente, e portanto, forjava uma situação de controle pelas regras impostas limitada àquele espaço vigiado.

Hoje, com a subversão do tempo e do espaço pelas redes, a vigilância assume posições menos evidentes, captando o que há de mais orgânico nas relações e comportamentos humanos, de modo que a conformidade em estar sendo vigiado não seja, propriamente, uma escolha pelo

[34] LYON, David. A cultura da vigilância: envolvimento, exposição e ética na modernidade digital. In: BRUNO, Fernanda *et al* (Org.). **Tecnopolíticas da vigilância: perspectivas da margem**. Tradução: Heloísa Cardoso Mourão et al.1ª Edição. São Paulo: Editora Boitempo, 2018 [2017], p.151-180.

medo. A autora Fernanda Bruno (2009; 2013) sugere o termo "vigilância distribuída" para explicar os processos reticulares, espraiados e imanentes[35], que operam sobre o comportamento humano por meio da captação de todo tipo de informação.

> **Proponho o termo vigilância distribuída como definição do estado geral da vigilância nas sociedades contemporâneas.** [...] Em linhas breves, **trata-se de uma vigilância que tende a se tornar incorporada a diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores**: nas medidas de segurança e circulação de pessoas, informações e bens; nas estratégias de consumo e marketing; nas formas de comunicação, entretenimento e sociabilidade; na prestação de serviços etc. **Nota-se que em certos casos ela se exerce misturada a dispositivos que não são prioritariamente voltados para a vigilância, sendo assim uma função potencial ou um efeito secundário de dispositivos que são projetados inicialmente para outras finalidades** – comunicação, publicidade, geolocalização etc. (BRUNO, 2009, p. 3, grifos nossos)[36]

O conceito elaborado pela autora é fundamental para o debate que propomos neste trabalho pois ela explica que, além de não haver um espaço ou um grupo restrito para a vigilância, todo tipo de ação, relação ou transação humana mediadas por aparatos tecnológicos produz rastros no ciberespaço, ampliando o espectro de controle não mais sobre um "grupo suspeito" mas sobre toda a sociedade.

Na percepção de Bruno, a informação, e não mais o medo, passa a ser a moeda de troca na prática dessa "vigilância para todos". A informação, muito melhor do que o medo, é matéria-prima para engendrar um conhecimento estruturado sobre os hábitos, o comportamento e até mesmo sobre as emoções humanas. Mas isso não significa que os sistemas de vigilância tenham abandonado totalmente o elemento "medo" como forma de legitimar a coerção. O medo ainda faz parte da fórmula da vigilância distribuída, que se apoia no tríplice discurso da segurança (onde o medo está), da visibilidade e da eficiência (BRUNO, 2009, p.3)[37] para legitimar sua prática.

---

[35] Op. Cit. BRUNO, 2013, p. 66-69.

[36] BRUNO, Fernanda. Mapas de crime: vigilância distribuída e participação na cibercultura. **Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação**. E-compós, v.12, n.2. Brasília: maio/ago, 2009, p. 1-16. Disponível em http://www.e-compos.org.br/e-compos/article/download/409/352. Acesso em 15 Jan 2021.

[37] Op. Cit. BRUNO, 2009, p. 1-16.

Sem embargo, a vigilância distribuída está integrada à economia e é legitimada por esta. Ela faz parte dos modelos de negócio, que atuam sob o manto da legalidade e da governabilidade, para capitalizar todo e qualquer tipo de informação. Assim, o uso de tecnologias para extração de dados mobiliza toda uma indústria da vigilância, em serviço do e com o Estado. Uma passagem de Lyon (2018), inclusive, nos lembra as revelações de Edward Snowden sobre os sistemas de espionagem estatais estadunidenses, que alarmaram o mundo na primeira década deste milênio.

> As divulgações de Snowden tornaram isso largamente claro, se antes restava alguma dúvida. Desde o princípio, em junho de 2013, os documentos de Snowden mostraram que a NSA tem acesso aos metadados de companhia telefônica (Verizon) e que também garimpa as bases de dados de clientes de empresas de internet como Apple, *Google*, Microsoft, Amazon e *Facebook* (por vezes mencionadas como as "Cinco Grandes"). Por um lado, portanto, essas empresas se envolvem com a vigilância de seus clientes em larga escala; por outro, elas partilham esses dados com agências governamentais (LYON, 2018, p.155)[38].

É sobre este cenário de mega estruturas tecnológicas e sistemas de vigilância, inclusive estatais, que a autora Shoshana Zuboff (2019)[39] elabora sua tese sobre a nova lógica de acumulação do capitalismo, que, segundo ela, se atualiza na dinâmica entre os processos informacionais e o avanço das tecnologias, usando a experiência humana como matéria-prima para acumulação de valor. No chamado "capitalismo de vigilância", a acumalação não mais se restringe aos ativos necessários para manter o fluxo de produção e consumo do mercado, mas a um banco de dados sem fim, o *Big Data*, capaz de tornar "monetizável" todo e qualquer conjunto de informações dele derivada.

O argumento central de Shoshana é que a galáxia de dados que hoje compõem o *Big Data* é operacionalizada de maneira intencional, irrestrita e irrefutável por mecanismos de inteligência artificial que não respondem a um hiper controlador, mas a diversos agentes controladores articulados, e cujas projeções não diferenciam as esferas do mercado e da segurança estatal[40]. No famoso texto "*Big Other: surveillance capitalism and the prospects of*

[38]Op. Cit., LYON, 2018 [2017], p.155.

[39] ZUBOFF, Shoshana. ***The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power***. New York: PublicAffairs, 2019.

[40] ZUBOFF, 2019 *apud* KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. **Revista Brasileira de Ciências Sociais.** V. 36, nº. 105, e3610514. São Paulo: ANPOCS, 2021, p.1-6. Disponível em https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-69092021000100702&lng=en&nrm=iso&tlng=pt. Acesso em 23 Jan 2021.

*an information civilization"* (2015), a autora já havia sinalizado para esse argumento quando discutiu os perigos dessa nova ordem de "poder soberano" para a democracia:

> O *Big Other* é o poder soberano de um futuro próximo que aniquila a liberdade alcançada pelo Estado de direito. É um novo regime de fatos independentes e independentemente controlados que suplanta a necessidade de contratos, de governança e o dinamismo de uma democracia de mercado. [...] Ao contrário do poder centralizado da sociedade de massa, não existe escapatória em relação ao Big Other. Não há lugar para estar onde o Outro também não está. (ZUBOFF, 2015, p. 44-45).

Nota-se, pois, que apesar de as prospecções da autora beirarem ao pessimismo apocalíptico sobre toda e qualquer interação humana mediada pela tecnologia, elas instigam um debate profundo e urgente sobre o futuro da Internet para a humanidade.

Afinal, se em algum momento da História a Internet abriu as possibilidades para um novo devir democrático através do acesso à informação e da comunicação horizontalizada, esse momento parece ter sido capturado por um outro devir: o de "abranger e revelar os amplos fatos imanentes de comportamentos econômicos, sociais, físicos e biológicos" (*idem*), cuja finalidade e interessados não sabemos claramente.

### 1.2.2 Tecnologias de vigilância e o controle dos corpos e da vida privada

Como visto na subseção anterior, os estudos contemporâneos têm alertado para como o uso das tecnologias nas interações sociais possibilitam a reorganização da vigilância, agora baseada em modelos descentralizados, e como isso amplia o poder de cooptação do Estado e das grandes corporações de tecnologia sobre o comportamento humano. Sendo um dos principais fatores que impulsionam esse modelo, a quase onipresença dos dispositivos tecnológicos na vida cotidiana abre precedentes para que qualquer aspecto da esfera pessoal ou social seja registrado e, por sua própria natureza, a vontade de exibição se transforme em objeto de visibilidade.

Por seu turno, a praticidade oferecida por esses aparatos tecnológicos nos conduz a uma conformidade ambivalente: "aceitar" o monitoramento das nossas rotinas em troca das facilidades que os serviços dispõem – como nos aplicativos de geolocalização, assistentes

virtuais, sistemas de automação residencial (IoT) e outros – mas também desfrutar da visibilidade que esses serviços projetam sobre a vida alheia.

Essa ambígua relação de troca estabelece, portanto, um circuito de vigilância capilarizado e eficiente, capaz de monetizar tudo o que há na interação sujeito-máquina, desde o uso de aplicativos domésticos até a comunicação, a sociabilidade, os corpos, os desejos, o pensamento.

A autora Paula Sibília (2016)[41] analisa tais circuitos sob a ótica da psicologia social, tentando entender como eles se articulam de dentro pra fora – isto é, do indivíduo para o social.

Para tanto, ela retoma o contexto de surgimento e popularização dos blogs e redes sociais, na primeira década dos anos 2000, e defende que aquele cenário fez criar uma espécie de "sujeitos narradores" – o "eu narrador" – da vida cotidiana.

Para a autora, a facilidade tecnológica de registrar e expor vida privada incentivou o que ela chama de "tiranias da intimidade na internet" (2016, p. 93)[42], "que compreendem tanto uma atitude de passividade e indiferença com relação aos assuntos de interesse público", quanto uma crescente concentração, nos espaços públicos, de conflitos íntimos. Logo, as tiranias da intimidade se apresentam como "gatilhos" – ou seja, respostas neurossensoriais a um estímulo externo – a serviço da vigilância e fazem com que o olhar sobre o outro torne-se a constante busca pelo entretenimento, mas também um exercício de controle.

Por outro lado, a compreensão de Sibília abre um caminho interessante para se pensar a exposição da intimidade como matéria-prima dos modelos de negócios impulsionados pelas *big techs* globais. Sobretudo as redes sociais, onde usuários compartilham abertamente informações pessoais e muitas vezes também utilizam para estabelecer relações íntimas, são espaços privilegiados para desestabilizar as hierarquias da vigilância, permitindo que a cessão e produção de informações sobre si seja uma prática voluntária e prazerosa.

---

[41] SIBÍLIA, Paula. Eu narrador e a vida como relato. In: SIBÍLIA, Paula. **O show do eu: a intimidade como espetáculo**. 2ª Edição. Rio de Janeiro: Contraponto, 2016, p.55-84.

[42] _____. Eu privado e o declínio do homem público. In: SIBÍLIA, Paula. **O show do eu: a intimidade como espetáculo**. 2ª Edição. Rio de Janeiro: Contraponto, 2016, p.85-124.

É, portanto, a partir das informações relacionais dos indivíduos – isto é, aquelas extraídas e processadas a partir das práticas pessoais e coletivas na Internet – que o mercado das *big techs* vai se munindo de dados e criando mecanismos eficientes para triagem, seleção e classificação de informações, com objetivo de perfilagem comportamental (*profiling*). Tais mecanismos, orientados por sistemas de inteligência artificial (IA), são capazes de assimilar os gatilhos emocionais, morais e linguísticos que orientam os diversos perfis comportamentais, e, a partir disso, induzir pequenas ações do cotidiano.

Assim, as corporações tecnologia têm investido em poderosas engenharias de *machine learning* ("aprendizagem das máquinas"), ou mais recentemente a *deep learning* ("aprendizagem profunda"), para agilizar e fragmentar ao máximo o nosso tempo de raciocínio sobre pequenas ações – tais como os cliques, as visualizações, os *likes* e afins – visando tornar cada vez mais automáticas as decisões sobre o consumo, o fornecimento de dados, as relações pessoais, a busca por conhecimento, e afins. Não apenas isso. A aprendizagem comportamental pode alcançar camadas ainda mais íntimas do ser humano. Ela dispõe também sobre nossos corpos.

Há um controle do corpo não-maquínico – ou seja, o corpo biológico – orquestrado por arranjos algorítmicos que reproduzem as desigualdades da sociedade disciplinar. Acobertados pelo discurso da segurança pessoal ou pública, convencionou-se aceitar o emprego de câmeras de reconhecimento facial, aparelhos de identificação biométrica, termômetros corporais, dentre outros, para o monitoramento e manutenção da ordem. Trata-se de uma evolução do biopoder, que alguns autores contemporâneos irão chamar de "biopolítica informacional" (FRAGA, 2006)[43], caracterizada pela demarcação dos corpos que podem morrer e dos que podem viver dentro da conformidade do capitalismo de vigilância.

Não faltam exemplos contundentes de que o uso de inteligência artificial para o aperfeiçoamento de sistemas preditivos – como o *data mining*[44], *data warehouse*[45] ou até

[43] FRAGA, Alex Branco. **Exercício da informação: governo dos corpos no mercado da vida ativ**a. Campinas: Autores Associados, 2006, 185 p.

[44] Trata-se de uma técnica de mineração de dados que busca fazer correlações mais difíceis ou ocultas em grandes volumes de dados.

[45] Trata-se de um tipo de automação para gerenciamento de banco de dados com grande volume e provenientes de várias fontes de sistemas, voltado para classificação de dados a partir de critérios de valoração pré-determinados

mesmo o polêmico uso de *dragnet surveillance*[46] – é a engrenagem para atualizar e manter os sistemas discriminatórios, com reflexos intencionais sobre a esfera criminal.

Nada parece escapar ao interesse da estratificação "dataísta", desde informações genéticas, raciais, de gênero e até de cunho religioso. Recentemente, uma interessante série chamada "*From Devices to Bodies*" (2021)[47] documentou casos em que a implementação de biotecnologias por empresas tem sido utilizada para a coleta de dados genéticos, visando a construção de uma espécie de "mapa de dados correlacionais" com aspectos envolvendo raça, gênero e território. O objetivo desse mapa não é esclarecido pelas empresas no documentário. Elas tampouco admitem que esse mapa existe.

Uma das pesquisadoras entrevistadas na série, Joy Buolamwini[48], do MIT, revela ter analisado os códigos dos sistemas de reconhecimento facial das empresas Face ++, IBM e Microsoft, e constatado que existe uma considerável soma de imprecisão no reconhecimento, apesar de essas empresas possuírem informações sobre os rostos da maior parte do mundo.

> Todas essas empresas detectam melhor rostos masculinos do que rostos femininos e em sujeitos claros que em peles escuras. Dados impressionantes da pesquisa mostram erros grotescos desses reconhecimentos faciais, com fotos antigas de mulheres negras, até mesmo de personalidades famosas, que não podem ser identificadas ou são identificadas com erros pelos sistemas (BUOLAMWINI, J. 2021. In: "*From devices to Bodies*", Fundação Heinrich Böll, Alemanha-Brasil-EUA: 2021)[49].

(por exemplo, valor monetário, valor ascendente, descendente, modelo, espaço temporal, etc). Tem sido muito utilizado pelas estratégias de *business intelligence* para estabelecer linhas de negócio.

[46] "*Dragnet*" é um tipo de sistema que pré-direciona medidas coordenadas para apreender criminosos ou suspeitos; incluindo barricadas de estradas e paradas de trânsito, testes de DNA etc, a partir de um "cálculo de incidência" que cruza dados como perfil bioantropológico, histórico criminal, geolocalização, entre outros, para orientar as rotas de atuação da polícia. O termo deriva de uma técnica de pesca, que consiste em arrastar uma rede desde o fundo do mar e trazê-la até uma área promissora de águas abertas. Nos EUA, o uso de sistemas preditivos, como o PredPol, é convencionalizado e geralmente são gerenciados por empresas privadas, autorizadas apenas a trabalharem com dados públicos - embora haja profundas discussões sobre a constitucionalidade desse recurso e se, de fato, as empresas usam somente informações públicas.

[47] Websérie produzida pela Fundação Heinrich Böll, no projeto "*Coding Rights*", explica como raça, gênero e território são percebidos por sistemas de reconhecimento facial desenvolvidos em diversos países do mundo. Disponível em https://br.boell.org/pt-br/2021/01/19/projeto-da-coding-rights-explica-como-raca-genero-e-territorio-sao-percebidos-pelo . Acesso em 25 Jan 2021.

[48] No segundo episódio da websérie, a pesquisadora Joy Buolamwini explica como funcionam os sistemas de reconhecimento facial da IBM, a Microsoft e da Face++. Disponível em https://www.youtube.com/watch?v=omP93gEuQfI&t=430s. Acesso em 25 Jan 2021.

[49] Transcrição de trechos da entrevista disponível em https://br.boell.org/pt-br/2021/01/19/projeto-da-coding-rights-explica-como-raca-genero-e-territorio-sao-percebidos-pelo . Acesso em 25 Jan 2021.

O estudo realizado por Buolamwini revela, ainda, que os sistemas de reconhecimento facial adjetivam os corpos com descrições como "seguro", "saudável" ou "mais inteligente" quase sempre relacionado à cor da pele identificada. A respeito desse ponto envolvendo a questão racial, insta salientar que há fortes debates na atualidade sobre o que os estudos de Ciências-Tecnologias-Sociedades (CTS) têm chamando de "racismo algorítmico".

Certamente, é tema que mereceria considerável aprofundamento neste trabalho, mas cujo embasamento teórico-metodológico da autora que o escreve ainda está em rasa construção. Contudo, não cedendo à sua complexidade, é fundamental apontar o diálogo entre as Teorias Raciais Críticas (TRC) e os Estudos de Vigilância como uma vertente transgressora para o debate sobre ética, biopoder e IA.

A autora Ruha Benjamin, na obra "*Race after Technology*" (2019)[50], expõe aquilo que, na sua visão, é mais controverso no uso de IA para o aperfeiçoamento da vigilância. Ela explica que todos os outros fatores que designam o capitalismo de vigilância foram atualizados conforme a nova lógica de domínio, menos a questão racial. Os modelos de negócio se reinventaram; a intervenção do Estado na vida privada se readequou; as redes sociotécnicas renovaram a padronização e os costumes nas relações sociais; mas o racismo continua como antes: fazendo refém os mesmos corpos, com as mesmas táticas, e de mãos dadas com os sistemas de justiça.

Ainda no bojo das questões éticas envolvendo o uso de tecnologia para o controle preditivo dos corpos, há uma questão importante sobre o lugar do consentimento para a coleta e tratamento de dados considerados sensíveis. Ao passo que há certa pressão por parte das organizações não-governamentais de direitos humanos no sentido de exigir maior transparência nas políticas de governabilidade de dados seguidas pelas empresas e pelo poder público – afinal, o que eles fazem com esses dados? –, há também constantes tentativas destes agentes de se desincumbir das restrições à guarda e tratamento de dados sensíveis pela alegação de que houve consentimento do titular.

---

[50] BENJAMIN, Ruha. ***Race after technology: Abolitionist tools for the new Jim Code***. Oxford (UK): Social Forces, 2019.

O pesquisador Bruno Bioni (2018)[51], uma das grandes referências sobre o tema no Brasil, tem reiterado que o consentimento pelo titular dos dados sensíveis não diminui a assimetria de poder que existe nas relações em que fornecer os dados pessoais seja condição para obtenção de algum benefício em contrapartida. Ele sinaliza que essa assimetria é muito sutil nas relações de consumo, porque nelas estabelecemos uma relação de escolhas, mas quando se trata das relações com o Estado, com quem congregamos uma relação de direitos e deveres, a desproporcionalidade fica mais evidente.

A provocação do autor evidencia uma importante ressalva, que se estende às possibilidades de regulamentação do uso de dados pessoais e sensíveis. Trata-se de um desafio que requer a análise casuística do fornecimento de dados para se avaliar quais eram as possibilidades de escolha do usuário dentro do cardápio de opções e, então, discernir o quão informado, consciente e livre foi o seu consentimento (2018, p. 197-198). Até porque, quem está em condições desiguais de poder, não tem como consentir. E, na espreita de regulamentação que estipule critérios de proteção ao mais vulnerável, o "mais forte" aproveita como pode.

Portanto, abordar a vigilância enquanto ponto de partida para o debate sobre a regulamentação de fenômenos emergentes na sociedade da informação é condição *sine qua non* para refletirmos e evitarmos as soluções desavisadas a respeito dos riscos e desafios inerentes à estrutura de poder que nos cerca.

Mesmo porque a vigilância nem sempre se apresenta como um problema para a maioria das pessoas, pois elas sequer conseguem dimensionar as consequências que a simples guarda de dados pode ter sobre suas vidas. Assim, uma lei cujo intuito seja criminalizar determinada conduta que oferece risco a um bem concreto, visível e mensurável dificilmente terá a mesma acepção de outra lei que proponha a proteção de metadados, para os quais a maioria dos cidadãos não faz ideia de quais bens podem ser decifrados e, portanto, violados a partir daqueles.

---

[51] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1ª Edição. Rio de Janeiro: Forense, 2018.

Com efeito, o fato de os debates regulatórios apontarem cada vez menos para uma formulação de direitos e garantias que protejam as singularidades e idiossincrasias dos sujeitos no cosmo da internet, é sintomático. Cada vez parece ser menos relevante a liberdade de "ser" e "existir" nos "espaços" revestidos pela plasticidade maquínica que emoldura as escolhas pessoais, e dispõe até mesmo sobre os corpos, como forma de externalizar uma personalidade identificável.

Por outro lado, o produto dos comportamentos não individualizáveis, mas identificáveis[52], parece ganhar o interesse das disputas por regulação e criminalização, deduzindo da vida privada pistas para a composição de um conhecimento coordenado sobre os [tipos de] "perfis" e, portanto, novas formas de monitoramento e controle sobre a vida.

E, visando entender como o Direito articula mecanismos de proteção a estes aspectos tão subjetivos e individuais, falaremos, a seguir, sobre a consolidação do campo da proteção de dados pessoais no Brasil.

## 1.3 Proteção de dados pessoais

Nas seções anteriores, vimos que o avanço da tecnologia possibilitou a formação de novas estruturas comunicativas pelo aumento do fluxo de informações, transformando, significativamente, a construção do conhecimento e a participação das pessoas na democracia. Não sem contexto, esses novos arranjos comunicacionais também provocaram mudanças importantes na relação entre Estado e cidadãos, e, alinhados ao crescimento das democracias liberais e à consolidação dos Estados de bem-estar social, deram outros contornos para a dicotomia entre público e privado.

Se no meado do Século XX a literatura distópica instigou o debate público ao denunciar mega-estruturas de controle que vigiavam o cotidiano das pessoas, como na metáfora do "*Big*

[52] Pablo Esteban Rodríguez propõe o conceito de "perfil dividual" a partir de dados pessoais identificáveis, que são usados pelas plataformas para a construção de um saber engendrado sobre "tipos de" indivíduos. Ver RODRIGUEZ, Pablo E. Espetáculo do dividual: tecnologias do eu e vigilância distribuída nas redes sociais. Tradução de María Sandra Arencón Beltrán e Marta Mourão Kanashiro. In: BRUNO, Fernanda *et al* (Org.). **Tecnopolíticas da vigilância: perspectivas da margem**. 1ª Edição. São Paulo: Editora Boitempo, 2018 [2015], p.182-198.

*Brother*" de Orwell[53], é também nesse contexto de ascensão das demandas pós-modernas que a proteção da vida privada alcança seu *status* de direito fundamental e, portanto, impõe a criação de mecanismos jurídicos vinculantes para limitar a interferência irrestrita do Estado na vida das pessoas.

Para nós, é importante pontuar alguns adendos sobre esse cenário – que de certo modo marca uma virada dogmática para a afirmação dos direitos de personalidade – porque é a partir da percepção da vida privada como bem tutelado que também a privacidade e, depois, a proteção de dados, ganhará importância no ordenamento jurídico. A seguir faremos um breve panorama de como esses conceitos foram se construindo no Direito.

### 1.3.1 Privacidade, intimidade e as bases para um direito fundamental autônomo

Em verdade, durante muito tempo a doutrina moderna discutiu se a expressão "vida privada" seria adequada para abranger as especificidades do que se pretendia consagrar como "direitos de personalidade" naquele contexto, mas após a menção expressa na Declaração Universal dos Direitos do Homem (ONU, 1948)[54] o termo "privacidade" ou "*privacy*" se afirmou como correlato do direito de proteção à vida privada.

Antes da DUDH colocar a privacidade como inerente à vida humana, o famoso artigo de Warren e Brandeis (1890), "*The right to privacy*"[55], comumente citado como obra precursora dos estudos na área, já trazia a percepção de privacidade enquanto direito humano marcado por um individualismo simplório. Isto é, como se a privacidade só se sustentasse, enquanto direito, se a liberdade do indivíduo em querer "estar só" fosse plena. Mas, apesar de a premissa do artigo ter se tornado antiquada com o passar do tempo, foi nele que, pela primeira vez, o direito

---

[53] ORWELL, George. **1984**. São Paulo: IBEP, 2003.

[54] ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em 12 Jan 2021.

[55] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v.4, n.5. BOSTON, US: 1890, sem paginação. Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em 12 Jan 2021.

à privacidade se distanciou da ideia de propriedade e se aproximou de valores mais complexos da vida cotidiana.

Ao explicar os valores aos quais o direito à privacidade foi se adequando ao longo do tempo, Danilo Doneda resgata a crítica de Stefano Rodotà, para quem o direito à privacidade contemporâneo está diretamente relacionado à estrutura de circulação e controle da informação. Segundo assinala nas premissas do escritor italiano, para entendermos substancialmente as projeções da privacidade na atualidade é necessário superar a percepção egoísta do *right to privacy* sem criar rupturas bruscas, admitindo-se que a atual ideia de privacidade não mais se baseia na mera acepção de "estar só" mas nas múltiplas relações entre "pessoas-informação-circulação-controle" (RODOTÀ, 1995 *apud* DONEDA, 2019, p.41).

Para o Direito, a ideia de Rodotà de reposicionar o entendimento sobre a privacidade é muito importante, pois ao mesmo tempo em que atualiza a dinâmica entre vida privada e processos comunicacionais, joga luz sobre outros elementos que dizem respeito às subjetividades da personalidade, mas que se diferenciam, na prática, do conceito de privacidade. Assim, elementos como a intimidade, a identidade pessoal, a honra, a dignidade, a integridade física, entre outros, deram substância ao reconhecimento da privacidade como direito fundamental, que, sobretudo após a segunda metade do século XX, ganhou a tutela constitucional em diversos países.

No Brasil, a Constituição de 1988 adotou, no inciso X do artigo 5º, a inviolabilidade "da intimidade", "da vida privada", "da honra" e "da imagem" como direitos fundamentais distintos e assecuratórios à dignidade da pessoa humana. Muito embora tal distinção pudesse restringir quais direitos de personalidade seriam tutelados, ao elencá-los no *hall* de direitos fundamentais o constituinte abriu possibilidades para sua garantia no plano prático, não apenas ligada à carga axiológica do princípio da dignidade humana mas também ao caráter de eficácia imediata, e portanto material, que eles possuem – um exemplo do que se convencionou chamar, em direito constitucional, de "abertura material do catálogo dos direitos fundamentais" (SARLET, 2001[56]), prevista no artigo 5º, parágrafo 2º.

[56] SARLET, Ingo W. **A eficácia dos direitos fundamentais**. 2ª. Ed. Porto Alegre: Livraria do Advogado, 2001. p. 97-102.

É bem verdade, porém, que a despeito dessa distinção expressa, os direitos de personalidade relacionados à vida privada, quais sejam, privacidade e intimidade, quase sempre estão juntos, cabendo à doutrina e à jurisprudência a tentativa de esmiuçar seus sentidos na prática. A esse respeito, em seu estudo sobre a recepção dos direitos de personalidade em perspectiva comparada com outros países, José Adércio Sampaio (1998)[57] sugere que a finalidade interpretativa da privacidade enquanto direito independente de outros correlatos (intimidade ou segredo[58]) não é provocar um problema dogmático para o Direito, mas considerar as particularidades e a variação de valores na construção dos sujeitos em cada tempo e sociedade.

A proposição de Sampaio, por sua vez, precede os debates sobre as urgências do nosso tempo informacional, tal como diversas pesquisas (LIMBERGER, 2000[59]; TEPEDINO, 2001[60]; RIBEIRO, 2002[61]; CARVALHO, 2003[62]; DONEDA, 2006[63]) começaram a pontuar a partir dos anos 2000. À época, tais pesquisas sugeriam que o *status* de direito fundamental era bastante amplo, e que sua aplicabilidade demandaria um profundo diálogo normativo com as inovações previstas no direito civil, no direito do consumidor, na segurança pública, no direito de família, entre outros. É também nesse cenário que as primeiras discussões sobre direitos de personalidade nas comunicações via Internet começam a chamar atenção, fazendo com que tanto a doutrina quanto a jurisprudência deixassem um pouco de lado a discussão terminológica (privacidade *versus* intimidade) e passassem a observar os rumos da legislação internacional para o assunto.

---

[57] SAMPAIO, José Adércio L. **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais**. Belo Horizonte: Del Rey, 1998, p.262-264.

[58] Sampaio faz referência à Teoria das Esferas (ou Teoria dos Círculos Concêntricos), elaborada por Heinrich Hubmann em 1953 e posteriomente utilizada pelo Tribunal Constitucional Alemão para definir níveis de privacidade. A teoria foi amplamente aperfeiçoada por doutrinadores ao redor do mundo que, de maneira resumida, avaliam o comportamento humano em três esferas: a esfera privada (mais externas), que engloba circunstâncias pessoais alheias ao conhecimento de terceiros; a esfera íntima (zona intermediária), que engloba valores ou informações restritas à algumas pessoas com as quais o indivíduo escolhe dividir; e a esfera do segredo (a mais interna), que é a zona do sigilo, das singularidades individuais. Portanto, sendo a privacidade o "círculo" mais externo, ela abrange todas as outras zonas, que são mais sensíveis e demandam uma proteção jurídica mais precisa.

[59] LIMBERGER, Têmis. A informática e a proteção à intimidade. **Revista de Direito Constitucional e Internacional**. v. 8, n. 33, Edição de Outubro a Dezembro. São Paulo: Revista dos Tribunais, 2000, p. 110–124.

[60] TEPEDINO, Gustavo. A tutela da personalidade no ordenamento Civil-constitucional brasileiro. In:_____. **Temas de direito civil. Rio de Janeiro**: 2001, p. 23-54.

[61] RIBEIRO, Luciana Antonini. A privacidade e os arquivos de consumo na Internet: uma primeira reflexão. **Revista do Direito do Consumidor**. V. 11, nº 41, Edição Janeiro a Março. São Paulo, 2002, p. 151-165.

[62] CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional. **Revista de Direito do Consumidor**, v. 46, Edição Abril a Junho. São Paulo, 2003, p. 77-119.

[63] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1ª Edição. Rio de Janeiro: Renovar, 2006.

Além dos já mencionados, outro fator que chamou atenção na primeira década do novo milênio foram as políticas de combate às desigualdades econômicas, sociais e culturais no Brasil, que incentivaram um novo perfil de consumidor no cenário da tecnologia: o cidadão comum conectado. O crescimento da indústria interna e a redução dos custos na produção de produtos de informática possibilitaram que mais pessoas tivessem acesso a estes produtos, aumentando, por consequência, a demanda pelo uso de internet.

Em 2005, 21% da população brasileira (32,1 milhões de pessoas)[64]acima de 10 anos de idade já tinham acesso domiciliar à internet, quando o uso de celulares ainda não era considerado para este fim. Em 2007, com a chegada dos *smartphones* e da internet móvel 3G, esse número sobe para 41%[65], atingindo, em 2014, a marca histórica de mais de 50% da população com acesso à internet móvel ou domiciliar (IBGE, 2015)[66]. Favorecido por esse contexto, diga-se, o aumento do uso de aplicativos de mensagens, blogs, redes sociais, e aplicativos de relacionamento causou uma verdadeira revolução na estrutura das relações sociais, influenciando progressivamente a relação das pessoas com a privacidade.

A autora Paula Sibília (2016), já mencionada na seção anterior, comenta que esses artefatos comunicacionais do mundo globalizado permitiram uma ressignificação gradual do conceito de esfera privada, fazendo com que a privacidade se confunda cada vez mais com a produção de dados sobre si para o mundo externo. Ela defende que o hábito de expor a vida privada propiciou pelo menos duas situações que tangenciam a discussão sobre a privacidade enquanto direito: (i) a banalização do fornecimento de informações pessoais em troca de acesso a serviços; e (ii) a falsa impressão de que os indivíduos podem, enquanto usuários, dispor sobre sua autonomia informativa.

---

[64] Informação disponível em https://censo2010.ibge.gov.br/noticias-censo.html?view=noticia&id=1&idnoticia=846&busca=1&t=ibge-contou-32-1-milhoes-usuarios-internet-pais . Acesso em 15 Jan 2021.

[65] Informação disponível em https://www.cetic.br/media/analises/destaques-tic-2007.pdf. Acesso em 15 Jan 2021.

[66] Informação disponível em https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/9564-pnad-tic-em-2014-pela-primeira-vez-celulares-superaram-microcomputadores-no-acesso-domiciliar-a-internet#:~:text=A%20PNAD%20TIC%202014%20investigou,ou%20em%20banda%20larga%20m%C3%B3vel.&text=Em%20termos%20absolutos%2C%20a%20conex%C3%A3o,9%25%20dos%20domic%C3%ADlios%20com%20Internet. Acesso em 15 Jan 2021.

Sobre o primeiro ponto, a voluntariedade no fornecimento de informações pessoais na Internet é matéria há muito discutida por Rodatà (2008)[67] pela ótica da vigilância. Para o autor, na medida em que não apenas o Estado, como também as empresas de tecnologia, detêm um conjunto sem fim de informações cedidas voluntariamente, abre-se precedentes para a violação de subjetividades inimagináveis das esferas da vida privada. Isso porque, por meio de simples informações sistematizadas, é possível estabelecer um conhecimento coordenado sobre o comportamento, os valores, e até os padrões de pensamento das pessoas, que poderão ser utilizados para finalidades diversas.

No mesmo sentido, a disposição da privacidade na sociedade da informação, voltando-se para aquilo que o próprio Rodotá denuncia, ganhou contornos próprios na discussão sobre direitos de personalidade, e avançou para uma nova categoria a ser tutelada: a autodeterminação informativa. Reconhecido pela primeira vez no julgamento do Tribunal Constitucional Alemão (1983)[68], o termo é inspirado nos princípios da "dignidade da pessoa humana" e do "livre desenvolvimento da personalidade" – ambos expressos na constituição alemã – e enfatizou a importância do dever de transparência dos agentes públicos no tratamento de dados pessoais dos cidadãos.

O entendimento firmado no julgamento foi no sentido de que não existem informações insignificantes, sobretudo quando estas podem compor um banco de dados articulado sobre os sujeitos, favorecendo aos agentes públicos o controle irrestrito sobre a vida das pessoas – característica, diga-se, dos governos totalitários. Logo, segundo a tese firmada, uma vez não havendo dados insignificantes ou neutros, a autodeterminação informativa estaria, necessariamente, vinculada à garantia de proteção dos dados pessoais.

Interessante observar que mesmo sendo uma construção conceitual que se formou na jurisprudência, a autodeterminação informativa influenciou, mais tarde, a doutrina e as legislações de vários países. Um dos primeiros resultados dessa repercussão foi a alteração da

---

[67] RODOTÀ, Stefano. **A vida na sociedade de vigilância. Privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 36-45.

[68] A decisão prolatada no processo que ficou conhecido como "Julgamento da Lei do Censo" (*Volkszählungsurteil* – 1 BvR 209/83, de 15.02.1983), discutiu a constitucionalidade de uma lei que permitia a coleta de dados dos cidadãos, sem consentimento, para troca de informações entre órgãos públicos.

Lei Federal de Proteção de Dados Alemã, em 1990, que trouxe o reconhecimento expresso da autodeterminação informativa enquanto fundamento da proteção de dados pessoais contra a iminência de projetos governamentais autoritários.

Naquele cenário, invocar o instituto da proteção de dados pessoais dava ao cidadão o poder de questionar a legalidade do uso de seus dados pelo poder público, independente de consentimento, funcionando, portanto, como um instrumento legal para a tutela da autodeterminação informativa. É bem verdade, porém, que fora da Alemanha a compreensão de ambos os conceitos foi se incorporando à ideia de que a proteção de dados, por si só, abrangeria o maior bem a ser tutelado - os dados pessoais. Mas, foi apenas no ano 2000 que essa consolidação doutrinária ganhou destaque na Carta de Direitos Fundamentais da União Europeia, elevando o direito à proteção de dados ao *status* de direito fundamental autônomo.

Do lado de cá do atlântico, todavia, a materialidade constitucional da proteção de dados demorou se afirmar, muito embora houvesse no ordenamento jurídico-normativo de alguns países americanos[69] referências consistentes à sua tutela no plano infralegal e até decisões judiciais no sentido de limitar ou ponderar seus efeitos quando em colisão com outros direitos fundamentais.

A esse respeito, Ingo Sarlet (2020)[70] comenta que da mesma forma que o direito das Américas foi influenciado pela construção dogmática europeia, hoje também o direito europeu se vê confrontado com desafios regulatórios que transcendem as fronteiras, o que "em searas como a tecnológica, a ambiental, a econômica e a comercial (e também o combate ao crime organizado, ao terrorismo etc)" revela a necessidade de se pensar a proteção de dados pessoais em sua "dimensão multinínel", isto é, a partir de parâmetros substancialmente comuns (mas

[69] Na obra "Tratado de proteção de dados pessoais" (2020) Danilo Doneda explica que a proteção de dados é discutida em países da América do Norte desde a década de 60, tendo sido os EUA o primeiro país a abrir uma discussão pública no sentido de propor a regulação do assunto para questões comerciais. Segundo comenta, as primeiras regulações teriam surgido no país em 1970, com o *Fair Credit Reporting Act* (FCRA), seguida do *Fair Information Practice Principles* em 1973, e do *Privacy Act* em 1974. DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: SCHERTEL MENDES, L. et al (Orgs.). **Tratado de proteção de dados pessoais**. (E-book não-paginado). Parte 1 - Fundamentos teóricos e históricos da proteção de dados pessoais. 1ª Edição. Rio de Janeiro: Editora Forense, 2020, sem paginação.

[70] SARLET, Ingo. W. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: SCHERTEL MENDES, L. et al (Orgs.). **Tratado de proteção de dados pessoais**. (E-book não-paginado). Parte 1 - Fundamentos teóricos e históricos da proteção de dados pessoais. 1ª Edição. Rio de Janeiro: Editora Forense, 2020, sem paginação.

também com a ressalva de eventuais peculiaridades), normativos e dogmáticos, para a solução dos problemas concretos" (2020, n.p).

Em linhas gerais, além dos já citados desafios inerentes ao seu reconhecimento enquanto direito universal e autônomo, hoje a proteção de dados abarca um campo multidisciplinar em matéria de direitos, que não deve prescindir da organização econômico-informacional das sociedades contemporâneas. Até porque, se num passado recente o Direito se ocupava em afirmar a importância da proteção dos dados para a garantia dos direitos personalíssimos em sua plenitude, agora, são urgentes as demandas para que não apenas as informações, como também o produto que elas geram, sejam tutelados perante à onipresente interação da vida privada com as atividades de controle e armazenamento realizadas pelas plataformas digitais.

A proteção de dados, portanto, representa a tutela das escolhas, do comportamento, das expressões e de todas as subjetividades que possam constituir o homem enquanto sujeito, pois, como há muito sinalizado por Rodotà (2008), a simbiose de esferas públicas e privadas no mundo conectado é um caminho sem volta. Cada vez mais "nós somos os nossos dados" (*sic*).

### 1.3.2 A tutela jurisdicional dos dados pessoais

Como visto na subseção anterior, a materialidade constitucional do direito à proteção de dados surge com a necessidade de solucionar impasses envolvendo direitos e garantias fundamentais, que, como tal, chegam à esfera jurisdicional. Na medida em que o conjunto de mecanismos legais, até então marcados pela carga principiológica dos direitos de personalidade, foram se mostrando insuficientes para a disciplinar questões mais sensíveis envolvendo ética e o uso de inteligência artificial no monitoramento das comunicações humanas, a judicialização de casos foi acompanhando a ideia – difundida sobretudo nos EUA – de que os dados pessoais são uma propriedade a ser tutelada e que sua violação deve ser reparada.

No Brasil, todavia, os dispositivos constitucionais que orientam a atuação jurisdicional permitem interpretações em pelo menos dois sentidos: (i) entender a proteção de dados como uma tutela inerente à dignidade da pessoa humana e à garantia dos direitos de personalidade –

ou seja, tutela de direitos absolutos e irrenunciáveis –; e (ii) entender que os dados são um conjunto de bens extrapatrimoniais, que envolvem direitos subjetivos e controversos quanto à sua disponibilidade[71] – como nos casos envolvendo a comunicação, a disposição do próprio corpo, uso de dados sensíveis e questões de bioética.

Em relação ao primeiro sentido, a tutela jurisdicional da proteção de dados encontra respaldo no núcleo duro dos direitos fundamentais (Artigo 5º, inciso X), sendo certo que, no que tange aos direitos de personalidade, a perspectiva personalíssima prevalece sobre a perspectiva patrimonial. Já o segundo sentido inclui elementos extrapatrimoniais que, na nossa Constituição, são abrangidos pela garantia de inviolabilidade do sigilo nas comunicações por correspondência, por vias telegráficas ou telefônicas e dos dados (Artigo 5º, inciso X), e pela vedação à disponibilidade do corpo, salvo em situações específicas de atendimento à saúde e à pesquisa científica, vedado em todos os casos sua comercialização (Artigo 199º, inciso 4º). O texto constitucional estipulou, ainda, o *Habeas Data* (Artigo 5º, inciso LXXII, regulamentado pela Lei Ordinária 9507/97) como instrumento próprio para o titular do direito pleitear o acesso e a retificação de seus dados pessoais disponíveis em banco de dados de uso público.

No plano infraconstitucional, o Código Civil de 2002 (Lei 10.406/2002) reproduziu nos Artigos 11 a 21 as garantias e o dever de proteção aos direitos de personalidade, ampliando-os quanto à descrição dos bens a serem tutelados – a honra, a imagem, a privacidade, a identidade pessoal, a integridade física, a autoria – e as violações cabíveis de reparação por danos morais ou materiais (Artigos 12 e 20, ambos do *caput* ao parágrafo único, do CC/2002).

Na mesma linha, o Código de Defesa do Consumidor (Lei 8.078/1990) já havia sinalizado a prevenção e a reparação de eventuais danos aos bens individuais como direitos basilares nas relações de consumo (Artigo 6º, inciso VI do CDC/1990), bem como previu expressamente que o acesso e a correção das informações pessoais constantes em banco de dados e em cadastro

[71] A esse respeito, Maria Celina BODIN DE MORAES (2010) sugere uma interpretação ampliada para a proteção de dados em vista da tutela dos direitos de personalidade, de modo a superar a visão limitada de proteção ao microcosmo da casa, onde se situam a intimidade e a privacidade, e estender a visão de que os dados são um elemento fundamental e inviolável para a liberdade das escolhas existenciais (BODIN DE MORAES, Maria Celina. Ampliando os direitos da personalidade. In: BODIN DE MORAES. **Na medida da Pessoa Humana - Estudos de direito civil-constitucional**. Capítulo II. 1ª Edição. Rio de Janeiro: Editora Renovar, 2010, p. 121-148. Disponível em https://www.researchgate.net/publication/288490662_Ampliando_os_direitos_da_personalidade . Acesso em 18 Jan 2021.

geral de consumidores é direito potestativo do consumidor, logo, sua violação é passível de pleito indenizatório na via judicial (Artigo 43 e incisos do CDC/1990).

Ainda sobre as medidas judiciais cabíveis para a tutela dos direitos individuais, dentre os quais se enquadram os direitos de personalidade e a proteção de dados, os Códigos de Processo Civil de 1973 e de 2015 dispuseram a antecipação de tutela (Artigo 273 no CPC/1973 e 300 no CPC/2015), medidas cautelares (Artigo 796 no CPC/1973 e 305 no CPC/2015) e a ação de obrigação de fazer (Artigo 287 e 461 no CPC/1973 e 497 no CPC/2015) como instrumentos hábeis a reparar ou "determinar providências que assegurem a obtenção de tutela pelo resultado prático equivalente" à sua reparação (vide redação do Artigo 497)[72].

Há de se salientar, todavia, que apesar de prestigiar a inafastabilidade da tutela jurisdicional para o pleno exercício dos direitos, o ordenamento brasileiro teve, sobretudo a partir da segunda década dos anos 2000, uma movimentação significativa de leis que incentivam a cultura do acesso e da transparência no uso de dados pelo poder público, e que dispõem de mecanismos administrativos para conter eventuais abusos.

São exemplos dessa tendência a Lei do Cadastro Positivo (Lei nº 12.414/2011), a Lei de Acesso à Informação (Lei nº 12.527/2011), o Marco Civil da Internet (Lei nº 12.965/ 2014) e o Decreto que instituiu a Política Nacional de Dados Abertos (Decreto nº 8.777 / 2016), que trazem recomendações expressas no sentido de reforçar o dever de publicidade quanto ao gerenciamento de dados pelos entes governamentais e, ao mesmo tempo, o dever de cautela quanto à confidencialidade das informações de cunho pessoal e dos dados sensíveis constantes nas bases de acesso público.

A partir de então, diversas resoluções normativas foram editadas no sentido de regular as peculiaridades atinentes ao uso e, principalmente, à disponibilização das informações pessoais detidas por agências reguladoras e por conselhos de área, compartilhadas com setores da

[72] Diz o Artigo 497 do Código de Processo Civil (2015): "Art. 497. Na ação que tenha por objeto a prestação de fazer ou de não fazer, o juiz, se procedente o pedido, concederá a tutela específica ou determinará providências que assegurem a obtenção de tutela pelo resultado prático equivalente. Parágrafo único. Para a concessão da tutela específica destinada a inibir a prática, a reiteração ou a continuação de um ilícito, ou a sua remoção, é irrelevante a demonstração da ocorrência de dano ou da existência de culpa ou dolo".

administração direta e organizações privadas. É o caso, por exemplo, da Resolução nº 2.227/2018 do Conselho Federal de Medicina (CFM)[73], que dispõe sobre o tratamento de dados pessoais "na prestação de serviços médicos mediados por tecnologias"; da Resolução nº 443/2019 da Agência Nacional de Saúde (ANS)[74], que trata "da implementação de programa de governança para gestão de riscos" envolvendo dados pessoais pelas operadoras de plano de saúde; e da recente Resolução nº 32/2020 do Banco Central (BC)[75], que institui "requisitos técnicos e procedimentos operacionais para a implementação do Sistema Financeiro Aberto (*Open Banking)*" no Brasil.

Bem se vê que, assim como ocorreu no contexto europeu, a regulação especializada da proteção de dados no Brasil se deu antes por atos normativos isolados e, após, pela necessidade de uniformização de seu entendimento no judiciário, como no caso da famosa Diretiva 46/95 do Parlamento e Conselho Europeu[76], cuja aplicação pelos tribunais em diversos países da Europa serviu de base para consagrar o Regulamento Geral de Proteção de Dados Europeu[77] ("GDPR", na sigla traduzida para o inglês), aprovado em 2016 e em vigor desde 2018.

Neste ponto, insta mencionar que desde a Constituição 1988 até o desenrolar de todo o conjunto de normas infralegais que incentivam a transparência e a governança sobre dados, um aparente conflito entre garantias individuais e interesse público chegou ao judiciário. Em 2015, o STF enfrentou o Tema de Repercussão Geral nº 483, no ARE 652777/ SP, que versava sobre possíveis riscos à privacidade, à intimidade e à integridade física de servidores públicos cujas

---

[73] A Resolução nº 2.227/2018 do CFM, também conhecida como "Regulação da Telemedicina", inspirou a "Lei do Prontuário Eletrônico" (Lei nº 13.787/2018), que também institui critérios específicos para o tratamento e guarda de dados pessoais e sensíveis. Disponível em https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/62181135 . Acesso em 12 Jan 2021.

[74] Disponível em https://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MzY3MQ== . Acesso em 12 Jan 2021.

[75] Disponível em https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=32 . Acesso em 12 Jan 2021.

[76] Considerada a primeira grande norma sistematizada e voltada para a regulamentação de matérias envolvendo proteção e tratamento de dados no plano transfronteiriço. Foi também a base normativa para a elaboração do Regulamento Geral de Proteção de Dados Europeu, que entrou em vigor em 2018. Disponível em https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046#:~:text=A%20Diretiva%2095%2F46%2FCE,da%20Uni%C3%A3o%20Europeia%20(UE) . Acesso em 12 Jan 2021.

[77] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&-from=EN. Acesso em 12 Jan 2021.

identificações pessoais (nome e CPF) e remunerações constavam no portal de transparência dos órgãos empregadores.

Na ocasião, o plenário entendeu, por unanimidade, que "é legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias", já que dizem respeito, antes de mais nada, a informações envolvendo gastos públicos e despesas orçamentárias. No tocante à proteção dos direitos de personalidade envolvidos, foram acolhidos os fundamentos do relator, Min. Teori Zavascki, o qual, citando precedentes do próprio Tribunal, destacou o seguinte:

> [...] 14. O meu voto já se percebe. A situação dos agravantes cai sob a regência da 1ª parte do inciso XXXIII do art. 5º da Constituição. Sua remuneração bruta, cargos e funções por eles titularizados, órgãos de sua formal lotação, tudo é constitutivo de informação de interesse coletivo ou geral. Expondo-se, portanto, a divulgação oficial. Sem que a intimidade deles, vida privada e segurança pessoal e familiar se encaixem nas exceções de que trata a parte derradeira do mesmo dispositivo constitucional (inciso XXXIII do art. 5º), pois o fato é que não estão em jogo nem a segurança do Estado nem do conjunto da sociedade. 15. **No tema, sinta-se que não cabe sequer falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo "nessa qualidade" (§ 6º do art. 37). E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor.** No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. Estado que somente por explícita enunciação legal rimada com a Constituição é que deixa de atuar no espaço da transparência ou visibilidade dos seus atos, mormente os respeitantes àquelas rubricas necessariamente enfeixadas na lei orçamentária anual, como é o caso das receitas e despesas públicas. [...]. (STF, Tema de Repercussão Geral nº 483 no ARE 652777/ SP, Relator: Min. Teori Zavascki, julgado em 23/04/2015, publicado em 01/07/2015 no DJE nº 128 , grifos nossos)[78].

É bem verdade, pois, que a discussão promovida no STF em 2015 ainda não havia encontrado o acalorado debate público sobre o que abrangeria, afinal, a privacidade dos dados pessoais como mais tarde a Ação Ordinária nº 2.367/2017, que pleiteou a suspensão da obrigatoriedade de divulgação da remuneração dos membros do Poder Judiciário pelo CNJ, encontrou. A causa de pedir na ação ordinária foi bastante parecida com a do ARE

[78] Trecho de autoria do Min. Ayres Britto no Agravo Regimental de Suspensão de Segurança AgMS 3.902/2011, citado pelo Min. Teori Zavascki, então relator do ARE 652777/ SP. Disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8831570 . Acesso em 12 Jan 2021.

652777/SP/2015, todavia, a Associação dos Juízes Federais do Rio de Janeiro e Espírito Santo (Ajuferjes), autora da ação, insistiu que "a indicação dos nomes e da lotação dos magistrados viola a intimidade e a privacidade desses agentes públicos" e que sua divulgação representaria verdadeira afronta às exceções previstas no artigo 4, incisos III e IV da LAI, que definem o que é informação sigilosa e de cunho pessoal[79].

Reafirmando os fundamentos da decisão de 2015, o então relator Min. Luís Roberto Barroso entendeu que o dever de publicidade e transparência também se aplica ao caso dos magistrados, "seja porque as informações sobre suas remunerações e proventos são de interesse coletivo e geral, o que atrai a regra do artigo 5º, inciso XXXIII da CRFB/1988", seja porque "não se enquadram na exceção de sigilo imprescindível às informações voltadas à segurança da sociedade e do Estado"[80]. Porém, no que dizia respeito à exceção de sigilo dos dados pessoais, o ministro afastou o argumento de que tais informações fossem consideradas "dados pessoais", visto que seriam decorrentes da natureza pública do cargo e não daquilo que a LAI definiu como "informação pessoal", qual seja "aquela relacionada à pessoa natural identificada ou identificável"[81].

Essa relativa inconsistência sobre o quê, afinal, estaria abrangido pelo conceito de "dados pessoais" foi um dos pontos que estendeu, desde 2012 até 2018, a aprovação de uma regulamentação geral para a proteção de dados no Brasil. Originada do Projeto de Lei Complementar nº 4060/12, que foi posteriormente apensado ao novo Projeto nº 53/2018 na Câmara dos Deputados, até finalmente ser aprovada no Senado Federal em julho de 2018, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) – dispõe sobre o conteúdo, quem são os titulares, o tratamento adequado, as medidas cabíveis à proteção, entre outros aspectos envolvendo a temática dos dados pessoais.

---

[79] De acordo com a LAI (Lei. 12.527/11): "Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: I - **observância da publicidade como preceito geral e do sigilo como exceção**; [...]" (Grifos nossos). No mesmo sentido, o Artigo 4º define: "Para os efeitos desta Lei, considera-se: [...] III - **informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado**; IV - **informação pessoal: aquela relacionada à pessoa natural identificada ou identificável** [...]". Texto literal disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm . Acesso em 18 Jan 2021.

[80] STF, AO 2367, Relator: Min. Luís Roberto Barroso, julgado em 13/03/2017, publicado em 27/08/2018 no DJE nº 176. Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5524489 . Acesso em 18 Jan 2021.

[81] Op. Cit. BARROSO, 2018.

Para delinear um conceito geral e harmônico com as legislações anteriores, a LGPD reproduziu, em seu artigo 5º, inciso I, o conceito de "dado pessoal" já previsto na redação do Artigo 4º, inciso IV da LAI e também avançou na definição das espécies de dados pessoais, quais sejam, os "dados sensíveis" (Artigo 5º, inciso II) e os "dados anonimizados" (Artigo 5º, inciso III). No artigo 12, parágrafo 2º, acrescentou que podem "ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada"[82]. Com relação ao tratamento dos dados pessoais considerados de interesse público, a aprovação da Lei enfrentou uma verdadeira disputa política a respeito de algumas obrigações consideradas excessivas[83] à Administração Pública e à Autoridade Nacional de Proteção de Dados (ANPD) e cujo embate acabou gerando uma grande "novela" para sua entrada em vigor, em setembro de 2020[84].

Assim, entre meandros envolvendo a vigência da LGPD e a definição da Autoridade Nacional de Proteção de Dados, em abril de 2020 o STF enfrentou novamente a controvérsia envolvendo a proteção de dados pessoais em conflito com disposições de interesse público, porém, dessa vez, numa situação bastante parecida com aquela que conferiu *status* de direito fundamental à "autodeterminação informativa" pelo Tribunal Constitucional Alemão.

A questão surgiu com o pedido de suspensão da eficácia da Medida Provisória nº 954/2020, que determinou o compartilhamento de dados dos serviços de telecomunicação, prestados por operadoras vinculadas à ANATEL, com o IBGE. Editada em 17 de abril de 2020 pelo então presidente, Jair Bolsonaro, a MP tinha como objetivo autorizar o acesso do IBGE aos nomes, telefones e endereço dos consumidores, com a justificativa de facilitar a produção de pesquisas oficiais durante o estágio de pandemia decorrente do COVID-19[85].

---

[82] Redação literal do artigo 12, parágrafo 2º da Lei 13.709/2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm . Acesso em 18 Jan 2021.

[83] As obrigações previstas nos artigos 23, inciso II; artigo 26, parágrafo 1º, inciso II; artigo 28, *caput* foram todas vetadas na Câmara dos Deputados por serem consideradas inconstitucionais face ao dever de transparência da Administração Pública, inclusive quanto à política de governança dos dados pessoais. As razões de veto estão disponíveis em https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html. Acesso em 19 Jan 2021.

[84] SENADO FEDERAL. "**Lei Geral de Proteção de Dados entra em vigor**". Notícia (online), publicada em 18 Set 2020. Disponível em https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor. Acesso em 15 Nov 2020.

[85] Em 26 de fevereiro de 2020, o Brasil confirmou o primeiro caso de infecção por coronavírus (COVID-19) em território nacional, dando início a uma das maiores crises de saúde pública da História. Em março o Senado

No dia 20 de abril foram apresentadas no STF as Ações Diretas de Inconstitucionalidade nºs 6387, 6388, 6389, 6390 e 6393, que solicitavam, desde logo, a suspensão cautelar da MP sob alegação de inconstitucionalidade por vício formal na proposição, ante à ausência dos quesitos de urgência e relevância (Artigo 62 da CRFB/88) e, no mérito, por violação aos dispositivos constitucionais de proteção à dignidade da pessoa humana (Artigo 1º, inciso III), à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (Artigo 5º, inciso X), do sigilo de dados (Artigo 5º, inciso XII) e da autodeterminação informativa – este último em referência ao já mencionado "julgamento sobre a Lei do Censo" alemão (1983).

Em 24 de abril de 2020, a relatora do caso, Ministra Rosa Weber, concedeu a cautelar, que foi, após, referendada no plenário por 10 votos a 1, suspendendo os efeitos da MP sob o seguinte fundamento:

> [...] O art. 2º da MP n. 954/2020 impõe às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, da relação de **nomes, números de telefone e endereços** de seus consumidores, pessoas físicas ou jurídicas. **Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII)**. **Sua manipulação e tratamento**, desse modo, **hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.** [...]. (STF, ADI 6387/DF, Relatora: Ministra Rosa Weber. Data de julgamento: 24/04/2020. DJE nº 102, publicado em 27/04/2020, grifos nossos)[86]

Neste cenário, não foram poucas as tratativas, sobretudo de doutrinadores e representantes da sociedade civil, no sentido de reconhecer a decisão do STF como uma virada paradigmática para a proteção de dados no Brasil. É bem verdade, porém, que o posicionamento do Tribunal muito se deve ao fato de que, à época, a LGPD ainda estava na *vacatio legis*[87] e,

---

reconheceu o Estado de Calamidade Pública, que se estendeu até dezembro daquele ano. Informação disponível em https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2020/03/entra-em-vigor-estado-de-calamidade-publica-no-brasil. Acesso em 18 Jan 2021.

[86] Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em 15 Dez 2020.

[87] Num breve resumo, a vigência da LGPD teve pelo menos três marcos temporais: (i) em 28 de dezembro de 2018, quanto aos artigos. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B;

na espera de uma tramitação formal no sentido de reconhecer a proteção de dados como um direito pleno, encontrou na técnica da mutação constitucional o caminho mais viável para adequar os princípios e valores da Carta Magna ao caso concreto, sem alterar sua redação literal.

A esse respeito, alguns doutrinadores consideram que houve um avanço na conduta do STF, sobretudo se tratando de um exercício interpretativo que mobilizou não apenas critérios hermenêuticos clássicos, como o da razoabilidade e da proporcionalidade, como também se esforçou para, em controle concentrado de constitucionalidade, afirmar a natureza supralegal da "autodeterminação informativa" em homenagem aos tratados e legislações internacionais já consolidados. Ingo Sarlet (2020) comenta que a decisão foi um passo um tanto atípico na atuação "desse STF atual" (sic), mas ainda assim positiva para a democracia brasileira. E explica:

> Ao passo que para o entendimento doutrinário dominante, os tratados de direitos humanos devem ter hierarquia normativa equivalente ao direito constitucional originário, situando-se no mesmo patamar, o STF, em que pesem os avanços a serem registrados, segue outorgando um *status* diferenciado aos direitos fundamentais da Constituição Federal em relação aos constantes dos tratados internacionais, que, a depender do caso, têm hierarquia equivalente à das emendas constitucionais (quando observado o rito previsto no parágrafo 3º do artigo 5º da CF), ou, não sendo essa a hipótese - o que vale para a quase totalidade dos tratados, em particular os que interessam à proteção de dados - hierarquia supralegal. (SARLET, Ingo W., 2020, n. p.)[88]

De fato, apesar de o julgamento de mérito quanto à inconstitucionalidade ter caducado, posto que a MP não foi convertida em lei dentro do prazo nonagesimal previsto no Artigo 62, parágrafos 3º e 7º da CRFB/1988, os pontos discutidos pelo Tribunal ainda fazem eco na tramitação de outros regulamentos que envolvem o uso público de dados pessoais, como mais adiante veremos ser o caso do Projeto de Lei 2630/2020 – o "PL das *Fake News*".

Primeiramente porque, a pretexto de ter sido editada no contexto da pandemia, a motivação institucional declarada na MP era bastante ampla e genérica – "facilitar a produção

(ii) em 1º de agosto de 2021, quanto aos artigos 52, 53 e 54; e finalmente (iii) em 14 de agosto de 2020, quanto aos demais artigos.

[88] SARLET, Ingo. W. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: SCHERTEL MENDES, L. et al (Orgs.). **Tratado de proteção de dados pessoais**. (E-book não-paginado). Parte 1 - Fundamentos teóricos e históricos da proteção de dados pessoais. 1ª Edição. Rio de Janeiro: Editora Forense, 2020, sem paginação.

de estatística oficial" – contudo sua relação com o cenário e finalidades específicas para o enfrentamento da pandemia causa pelo COVID 19 não estavam descritas no texto.

Além disso, a medida solicitava o compartilhamento de dados de todos os consumidores brasileiros das referidas empresas de telecomunicação, chamando atenção pelo contraste em relação à metodologia geralmente utilizada pelo IBGE, que na PNAD, por exemplo, utiliza dados amostrais de pouco mais de 210 mil domicílios brasileiros[89].

Outro ponto de suma importância abordado no julgamento da MP é a questão da segurança da informação. Conforme, inclusive, questionado na ADI 6387 o texto da MP não previu qualquer medida que estipulasse o tratamento adequado na transferência e armazenamento dos dados dos milhões de consumidores. A ausência de um dispositivo rígido neste sentido, diga-se, causou estranhamento, sobretudo após diversos episódios de vazamentos de dados e ataques aos servidores de instituições públicas e privadas.

Por fim, a edição de uma MP, cuja tramitação é célere e possui eficácia imediata, por si só trouxe questionamentos sobre a necessidade de uma discussão mais apurada sobre um assunto envolvendo os direitos individuais de milhões de brasileiros. Ainda mais se considerado que, até o início deste ano de 2021, está em curso no Congresso Nacional a Proposta de Emenda à Constituição n° 17 de 2019 (PEC 17/2019)[90], com o objetivo de "incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais".

Mas, enquanto a consolidação constitucional não avança pelo rito formal, o que talvez fique de mais relevante na discussão promovida no STF é o entendimento de que a proteção de dados é um microssistema de direitos, que, como tal, engloba outros direitos individuais e coletivos; que pode ser demandado por seus titulares ou outros legitimados; e que possui regulamentação e princípios próprios compatíveis e complementares à Constituição.

---

[89] Em 2019, a PNAD contínua utilizou uma amostra de 211.334 mil domicílios por trimestre, considerando todas as cinco macrorregiões do país (IBGE. Pesquisa Nacional por Amostra de Domicílios Contínua - Notas técnicas - Versão 1.6. Capítulo "Tamanho da amostra". Rio de Janeiro: Ministério da Economia, 2019, p. 10). Disponível em https://biblioteca.ibge.gov.br/visualizacao/livros/liv101674_notas_tecnicas.pdf . Acesso em 12 Jan 2021.

[90] Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em 18 Jan 2021.

A proteção de dados, portanto, é um terreno fértil para pensarmos diversas problemáticas da sociedade da informação e antever, por exemplo, o cenário que se desenha sobre a questão da desinformação, conforme abordaremos a seguir.

# 2. REGULAR O MODERADOR, MODERAR O (QUE É) REGULADO

O ano de 2020 trouxe novos contornos para o debate sobre desinformação no Brasil, que já estava sendo pautado pelo conturbado clima de "pós-eleição" instalado no país desde 2018. Em meio a disputas políticas pelo direito de definir o quê eram e como coibir as "*Fake News*", pelo menos três projetos de lei foram apresentados na Câmara dos Deputados e no Senado, tendo sido o PL 2630/2020 o que mais se sustentou na tramitação legislativa até então.

A proposta, que teve como foco identificar condutas consideradas “inautênticas” e adotar sistemas preventivos de combate à desinformação, levantou dúvidas sobre como conciliar o objetivo de responsabilizar provedores e usuários sem afrontar princípios já consolidados no Marco Civil da Internet e na Lei Geral de Proteção de Dados. Além disso, a velocidade com a qual a proposta foi lançada e o sensível momento de retração da participação civil em decorrência dos problemas da pandemia, fizeram com que o debate sobre a regulamentação ocorresse de maneira bem diferente do MIC.

Se no MCI os desafios da regulamentação estavam em pautar a neutralidade da rede, tendo a responsabilização civil e a segurança cibernética como paradigmas, hoje o maior desafio da regulação da desinformação está em regular o dever de transparência nas políticas de moderação dos intermediários, tendo também a proteção de dados pessoais como paradigma.

E é visando explorar os significados possíveis para esta “moderação regulada” que o título deste capítulo propõe um jogo de palavras: moderar no sentido de impor critérios para o controle, já que a regulação nos parece o caminho mais democrático para conciliar direitos e avanços tecnológicos; e moderar no sentido de adequar, às justas proporções, medidas que sejam convenientes a todos os interesses.

Assim, longe de defender intervenções sobre os modelos de negócio ou, ao contrário, o completo esvaziamento regulatório, a moderação aparece, neste trabalho, como um desafio para o exercício da cidadania que requer, em boa medida, entender a história e as problemáticas da regulação da Internet até agora. Passemos, então, a algumas delas.

## 2.1 Marcos regulatórios (para o uso) das plataformas digitais no Brasil

Para muitos estudiosos do Direito Digital no Brasil, o Marco Civil da Internet (Lei 12.965/14) é o início da estrutura de princípios norteadores, garantias, direitos e deveres do campo, que têm na Internet o seu "tempo" e "espaço" de operabilidade. Tido como exemplo de procedimento regulatório, que utilizou as redes para abrir e ampliar a participação cidadã no processo legislativo, o MCI é uma carta principiológica, que conseguiu unificar em um só "código" ideias favoráveis à liberdade, à responsabilização civil; à ética e à segurança na Internet. Assim também o descrevem Ronaldo Lemos e Carlos Affonso Souza, dois principais autores do anteprojeto que deu origem ao MCI:

> Distanciando-se assim de uma regulação repressiva da rede, o Brasil ofereceu um dos mais simbólicos exemplos que anima os debates globais sobre uma regulação da rede que tenha os direitos humanos como o seu fio condutor e que mantém o caráter principiológico para evitar uma caducidade precoce de seus dispositivos. (LEMOS&SOUZA, 2016, p. 16)[91]

De fato, o MCI foi a proposta mais consensual que, na história recente, teve a ambição de regular o uso da Internet no Brasil, mas não foi a primeira. Cabe lembrar, numa breve passagem de tempo, que sua proposição resultou das discussões iniciadas na Câmara ainda em 2009, após diversas audiências públicas, propostas de emenda, pressão política envolvendo suspeitas de espionagem nas comunicações eletrônicas de chefes do Estado[92] e todo um iminente cenário de legislações especializadas que surgiam, sobretudo no campo penal, para regular o uso de plataformas digitais e Internet no Brasil.

Na seara penal, as discussões sobre a regulação foram precedidas pelo polêmico PL 89/2003 (antes PL 84/99), proposto pelo então Senador Eduardo Azeredo, cujo debate se arrastou durante anos no Congresso devido às críticas à tentativa de cercear a liberdade de

---

[91] LEMOS, Ronaldo; Carlos Affonso SOUZA. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016,P. 16-17. Disponível em https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em 15 Jan 2021.

[92] SENADO FEDERAL. "**Marco Civil da Internet foi reação brasileira a denúncias de Snowden**". Notícia publicada em Jul 2014. Disponível em https://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/propostas-senadores-querem-inteligencia-forte/marco-civil-da-internet-foi-reacao-brasileira-a-denuncias-de-snowden . Acesso em 12 Fev 2021.

expressão e criminalizar toda e qualquer atividade *hacker*[93]. Apelidado de "AI-5 Digital", o projeto tentava definir condutas como "difusão de vírus", "acesso não autorizado" e "*phishing*" como tipos penais de crimes eletrônicos.

Mais tarde, em 2006, o Senador retirou tais definições do projeto e sugeriu mais responsabilização aos provedores. As alterações resultaram na aprovação, em 2012, da "Lei de Cibercrimes" (Lei nº 12.735/12), também conhecida como "Lei de Azeredo", que, apesar de ter entrado em vigor na sua versão reduzida, contribuiu para uma importante classificação doutrinária[94] dos crimes digitais: (i) crimes digitais próprios, que são aqueles que por terem natureza "digital", mobilizam algum risco informático à coletividade, quais sejam, disseminação de vírus, invasão de sistemas, entre outros; e (ii) os crimes impróprios, que são aqueles que já existem no mundo material e são facilitados pela utilização de equipamentos eletrônicos, como os crimes de extorsão, estelionato e pedofilia, por exemplo.

No mesmo propósito, com as devidas ressalvas, pode-se dizer que a Lei de Azeredo também foi precursora na definição de algumas condutas consideradas importantes para a proteção de dados pessoais, tais como: obtenção, transferência ou fornecimento não-autorizado de dados eletrônicos e divulgação ou utilização indevida de informações e dados pessoais.

Importante lembrar que antes de haver legislação especializada, as sanções destinadas a punir quem praticava crimes informáticos eram associadas ao artigo 163 do Código Penal de 1940, destinado a tutelar apenas bens materiais contra as condutas de "destruir, inutilizar ou deteriorar" pertence alheio. Ou seja, enxergava-se a segurança na rede como uma questão eminentemente patrimonial. Aprovada no mesmo contexto da Lei Azeredo, a Lei 12.737/2012, apelidada de "Lei Carolina Dieckman", muda essa lógica na medida em que coloca a violação dos dados informáticos também atrelada à intimidade, à privacidade e à honra, isto é, alcançando a esfera dos crimes contra a pessoa – algo que só era feito, no ambiente digital, quando se tratava de calúnia, difamação e injúria (artigos 138, 139 e 140 do Código Penal) publicadas em veículos de comunicação.

---

[93] ESTADÃO. "**Lei Azeredo propõe combate a Hackers**". Notícia publicada em 28 Jun 2011. Disponível em https://link.estadao.com.br/noticias/geral,lei-azeredo-propoe-combate-a-hackers,10000038992. Acesso em 12 Fev 2021.

[94] VIANA, Tulio. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003, p. 13-26.

Há de se revisar que a pretensão de regular atividades intermediadas pela internet também pautou outras áreas do Direito que, desde o início dos anos 90, possuem alguma medida relacionada ao tema. No Direito Comercial uma das primeiras leis que dispunha sobre a comercialização de produtos eletrônicos, incluindo *softwares*, no setor da informática e automação, a "Lei de Informática" (Lei nº 8.248/1991), teve sucessivas atualizações dadas pelo Decreto 5.906/06 e pelas Leis nº 10.176/01, Lei nº 13.674/18 e Lei nº 13.969/19). No Direito tributário, a Lei nº 947.2/1997, conhecida como "Lei Geral das Telecomunicações" foi uma das primeiras a versar sobre modelos de tributação aos serviços prestados por provedores de Internet, que à época era considerada como uma coisa, um produto.

No Direito Eleitoral, a Lei nº 10.740/2003 implantou o sistema de identificação digital do voto (as urnas eletrônicas), que serviu de base para a Lei nº 12.034/2009, que alterou a "Lei das Eleições" (Lei nº 9.504/1997), permitindo a realização de campanhas eleitorais na Internet. No Direito Processual, a "Lei do Processo Eletrônico" (Lei nº 11.419/ 2006) instituiu a informatização dos processos judiciais e tratou, dentre outros pontos, da questão da segurança dos dados e integridade das informações constantes dos autos eletrônicos. No Direito Consumerista, o Decreto 7962/2013, dispôs sobre a contratação no comércio eletrônico, regulamentando o Código de Defesa do Consumidor (Lei 8.078/1990) e a posterior Lei do Cadastro Positivo (Lei 12.414/2011).

Bem se vê que logo na primeira década dos anos 2000, o Brasil já dispunha de um considerável conjunto de legislações sobre a governança da Internet em diversos campos de atuação, muito embora essa não tenha sido a tendência ao redor do mundo. Isso porque, sobretudo nos países com forte influência liberal-econômica, a discussão sobre regular ou não a Internet enfrentou muitos entraves, o que acabou fazendo com que a regulamentação ocorresse, em grande medida, por meio do controle judicial, interpretações principiológicas constitucionais ou instrumentos infralegais (instruções normativas ou portarias).

Apesar de ter saído na dianteira destes debates, o Marco Civil importou alguns fundamentos anacrônicos baseados em "políticas de moderação das telecomunicações", que surgiram nos EUA no final dos anos 90 para tratar da responsabilização civil dos provedores nos casos em que os conteúdos produzidos por terceiros violassem os termos de moralidade,

previstos no "*Communications Decency Act*" (CDA, 1996) [95] – algo como um código de conduta moral que pretendia combater a pornografia nos meios de comunicação – , e de autoria, previstos no *Digital Millennium Copyright Act (*DMCA, 1998)[96] – Lei de Direitos Autorais. Basicamente, surge neste contexto a ideia de que os *media* não podem ser responsabilizados pelo que transmitem ou publicam, mas têm o dever de "remover" os conteúdos considerados inadequados.

Essa discricionariedade, também conhecida como "autorregulação dos provedores", causou bastante polêmica nos EUA já no início dos anos 2000, porque se revelava incompatível com a liberdade de expressão e de manifestação do pensamento, cujo debate terminou por promover o sistema de *notice and take down* também na esfera digital , isto é, os provedores só responderiam pelos conteúdos indevidos se, uma vez notificados (*notice*) pelos autores lesados ou pela polícia, não tomassem medidas para a retirada (*takedown*).

Para os provedores, esse modelo trouxe uma espécie de blindagem contra o dever de indenizar porque convencionou a prática de retirar o conteúdo indevido tão logo recebessem qualquer notificação de irregularidade. Por outro lado, também favoreceu uma verdadeira guerra de "censuras" na medida em que o crescente número de casos de denunciação falaciosa começou a obstar, inclusive, a veiculação de conteúdos legítimos.

Apesar da controvérsia, fato é que o *notice and take down* vem sendo adotado e adaptado em diversos países: nos EUA, a notificação de conteúdos ilícitos enseja o dever de remoção pelos provedores, porém eles se reservam o direito de informar ao denunciante que, em caso de denúncia falsa, poderá responder por perjúrio, sem prejuízo do direito à contra-notificação. No Canadá, o modelo de *notice and notice*[97] prevê que, uma vez notificados pelos titulares do direito autoral, os provedores devem também notificar os usuários do serviço, alertando-os de que o consumo de conteúdo suspeito pode vinculá-los a atividades infratoras.

---

[95] CDA. "***Communications Decency Act***" (1996). Disponível em https://www.law.cornell.edu/uscode/text/47/230 . Acesso em 12 Fev 2021.

[96] DMCA. "***Digital Millennium Copyright Act***" (1998). Disponível em https://www.copyright.gov/legislation/dmca.pdf. Acesso em 12 Fev 2021.

[97] A Lei de Direitos Autorais do Canadá que exige que intermediários da Internet, como Provedores de Serviços de Internet (ISPs), encaminhem notificações de proprietários de direitos autorais para assinantes de Internet, alertando-os de que suas contas de Internet foram vinculadas a supostas atividades infratoras, como o download ilegal de filmes. Informação disponível em https://www.ic.gc.ca/eic/site/Oca-bc.nsf/eng/ca02920.html. Acesso em 12 Fev 2021.

Há ainda modelos híbridos, como os da França e da Espanha, que até bem pouco tempo adotavam medidas de "resposta gradual" (*three-strikes*) às violações ocorridas na rede. Neste modelo, o provedor tem o dever tornar o conteúdo ilícito "identificável" para monitorar quem o acessa e, assim, avisar o usuário de que ele pode ser responsabilizado pelo seu consumo; caso o usuário queira prosseguir na ação, o provedor pode suspender o serviço, aplicar multa ou endereçar o caso às autoridades policiais[98].

Na América Latina, o Brasil e o Chile são exemplos de países que, além de terem uma legislação estruturada sobre o assunto, adotaram o modelo de *judicial notice and take down*, por meio do qual um conteúdo pode ser "retirado" ou "suspenso" da plataforma somente após apreciação judicial, sob pena de violação ao princípio constitucional da liberdade de expressão. Tal previsão foi positivada nos artigos 19, 20 e 30 do MCI, que se concentraram em disciplinar os critérios para a reserva de jurisdição e as obrigações decorrentes para os provedores.

A eficácia destes modelos de responsabilização de intermediários no mundo ainda enfrenta muitas discussões, já que os avanços tecnológicos e os fenômenos culturais na rede têm desconfigurado, cada vez mais, a lógica da autonomia da ação e da legitimidade da autoria na Internet.

De todo modo, o que se tem em consenso hoje é que, independente de notificação do autor ou da autoridade judicial, as plataformas devem criar mecanismos para evitar que conteúdos ilícitos sejam veiculados, sob pena de responderem pela ausência de precaução. Trata-se de um novo modelo de regulação, chamado de *notice and stay down*, recentemente adotado pelos países da União Europeia na Diretiva 2016/0280-2019[99], que consiste em incentivar os provedores a usarem algoritmos e "filtros de conteúdo", visando obstar a veiculação do conteúdo indevido na origem (*upload*) e dificultar, inclusive, que ele seja postado novamente.

---

[98] SOUZA, Rebeca H. V. de; SOLAGNA, Fabrício; LEAL, Ondina F. As políticas globais de governança e regulamentação da privacidade na internet. **Revista Horizonte Antropológico**, v. 20, n. 41, Junho de 2014. Porto Alegre: IFCH-UFRGS, 2014, p. 141-172. Disponível em https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-71832014000100006. Acesso em 12 Fev 2021.

[99] UE. **Diretiva 2016/0280**, de 15 Abr 2019. Disponível em https://data.consilium.europa.eu/doc/document/PE-51-2019-INIT/en/pdf. Acesso 12 Fev 2021.

Notadamente, a discussão a respeito dos modelos regulatórios esteve, durante muito tempo, permeada pela preocupação com os direitos autorais, sendo certo que as medidas adotadas até então alteraram a forma como se usa a Internet, especialmente para o consumo de produtos culturais e uso de redes sociais. Todavia, no tocante aos fenômenos culturais e novos riscos emergentes, essas discussões ainda parecem enfrentar desafios para conciliar os princípios já consagrados – dentre os quais destaca-se a neutralidade da rede, a liberdade de expressão e a proteção de dados – com os modelos de negócio em avanço.

No Brasil, essa tem sido uma preocupação sistêmica desde que a promulgação da Lei Geral da Proteção de Dados (2018), que incorporou os princípios basilares do MCI, reacendeu o debate sobre a responsabilização dos intermediários em casos envolvendo uso irregular de dados pessoais, vazamentos, veiculação de notícias falsas e discurso de ódio, sobretudo no cenário eleitoral.

A exemplo do que veio à tona em 2018, no escândalo envolvendo o *Facebook* e a empresa de consultoria *Cambridge Analytica*[100], acusada de ter coletado indevidamente os dados pessoais de 50 milhões de usuários para impulsionar conteúdos segmentados por perfil nas eleições presidenciais estadunidenses de 2016, incluindo notícias falsas, vemos o quanto esse debate da proteção de dados nas plataformas tangencia, também, o enfretamento da desinformação.

Cabe lembrar que o caso da *Cambridge Analytica* ganhou repercussão transnacional, tendo o *Facebook* sido responsabilizado pelo vazamento dos dados – mas não pela propagação de conteúdo falso – inclusive no Brasil[101], com base nos princípios da "preservação e garantia da neutralidade de rede" e da "proteção dos dados pessoais", ambos previstos no artigo 3, inciso III e IV do MCI , já que a ANPD e as sanções previstas na LGPD só entrariam em vigor em 2020. No mesmo propósito, em 2019 o Congresso Brasileiro instaurou a "CPI das *Fakes*

[100] THE GUARDIAN. "***Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach***". Notícia (online) publicada em 17 Mar 2018. Disponível em https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em 12 Fev 2021.

[101] EBC. "**Ministério multa *Facebook* por abuso no compartilhamento de dados**". Notícia (online) publicada em 30 Dez 2019. Disponível em https://agenciabrasil.ebc.com.br/geral/noticia/2019-12/ministerio-multa-facebook-por-abuso-no-compartilhamento-de-dados. Acesso em 12 Fev 2021.

*News*"[102] para apurar denúncias de impulsionamento indevido de conteúdo eleitoral, propagação de notícias falsas, discurso do ódio e assédio virtual durante as eleições presidenciais de 2018.

Em 2020, a CPI teve seu curso prorrogado para investigações sobre desinformação a respeito do coronavírus e discursos de negacionismo epidemiológico, o que, possivelmente, contou com a ajuda das condutas públicas[103] do então Presidente da República, Jair Bolsonaro. Até a conclusão deste trabalho, as investigações ainda estavam em curso.

Conforme visto, no tocante às diversas problemáticas envolvendo o uso da Internet, as propostas regulatórias no Brasil e no mundo continuam enfrentando polêmicas a respeito dos limites de responsabilização dos intermediários frente aos abusos cometidos por terceiros, contudo, o consenso em torno do dever de preservação da neutralidade da rede e da privacidade dos dados pessoais é o que tem prevalecido.

No Brasil, desde o início de 2020 alguns projetos de lei se propuseram a superar os entraves do modelo de autorregulação com vistas ao que tem sido chamado de "autorregulação-regulada" ou "corregulação". Neste modelo, o dever de transparência dos provedores nas suas políticas de moderação e tratamento de dados pessoais é o ponto central na discussão sobre responsabilização.

Conforme a experiência já adotada na Alemanha desde 2017[104], a "autorregulação regulada" pressupõe que as diretrizes para a identificação, notificação, remoção e processamento do contraditório façam parte da cultura de uso das Redes, sendo os provedores (não todos, apenas os que possuem mais de 2 milhões de usuários) responsáveis pela identificação dos conteúdos ilícitos a partir de um rol previamente estipulado na lei; pela retirada do conteúdo após notificação; pela coordenação do procedimento de defesa prévia e

---

[102] SENADO FEDERAL. **Comissão Parlamentar Mista de Inquérito - *Fake News***. Instaurada em 04 Set 2019. Disponível em https://legis.senado.leg.br/comissoes/comissao?1&codcol=2292. Acesso em 12 Fev 2021.

[103] AOS FATOS, Agência de *Fact-Cheking*. "**Bolsonaro nega orientações da ciência e distorce informações para minimizar pandemia**". Checagem (online) publicada em 24 de março de 2020. "Disponível emhttps://www.aosfatos.org/noticias/bolsonaro-nega-orientacoes-da-ciencia-e-distorce-informacoes-para-minimizar-pandemia/. Acesso em 12 Fev 2021.

[104] ALEMANHA. ***Neztdurchsetzungsgeset - NetzDG***. "Lei de Fiscalização da Rede". Aprovada em 09 Jul 2017. Disponível em https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Acesso em 12 Fev 2021.

posterior à retirada; pela elaboração de relatórios periódicos a respeito dos casos detidos e em suspeição e, por fim, pelo envio de relatórios periódicos ao órgão de regulação estatal, responsável por validar todas as etapas da moderação. Somente em caso de irregularidades apontadas pelo órgão de regulação, encaminha-se a controvérsia ao judiciário.

Por pretender implantar uma cultura de moderação "mais moderada", este modelo se coaduna com algumas propostas alternativas orientadas por acadêmicos, ativistas e organizações civis de todo mundo, no sentido de que a regulação deve ser pautada por princípios e medidas que favoreçam a diversidade do ambiente informacional, e não o oposto.

São exemplos dessas propostas a carta de Princípios de Manila sobre Responsabilização de Intermediários (2015)[105], a carta de Princípios de Santa Clara sobre Transparência e *Accountability* na Moderação de Conteúdo (2018)[106] e o Código de Conduta Sobre Desinformação da União Europeia (2018)[107] que, em linhas gerais, sugerem caminhos para a adequação universal da neutralidade da rede, dentre as quais destaca-se: priorizar a visibilidade e transparência das políticas de governança de dados das empresas; priorizar a privacidade do usuário desde a concepção (*Privacy By Design*) como regra universal, a qual pressupõe exceções que devem ser reguladas por lei e adequadas conforme a permissão do usuário (*Privacy By Default*) e incentivar a criptografia ponta-a-ponta, garantindo a segurança dos dados durante todo o ciclo informacional.

É possível dizer que a movimentação em torno de tais propostas, além das problemáticas envolvendo irregularidades em campanhas eleitorais em diversos países, tenha contribuído para acelerar o debate sobre a regulamentação da desinformação no Brasil, que têm no PL 2630/2020, o "PL das *Fake News*", a discussão mais avançada até então. Vejamos a seguir quais os principais desafios desse projeto.

---

[105] FILIPINAS. **Princípios de Manila sobre Responsabilização de Intermediários**. Publicado em 30 Mai 2015. Disponível em https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf. Acesso em 12 Fev 2021.

[106] EUA. **Princípios de Santa Clara sobre Transparência e Accountability em Moderação de Conteúdo**. Publicado em 7 Mai 2018. Disponível em https://santaclaraprinciples.org/. Acesso em 12 Fev 2021.

[107] UE. **Código de condutas sobre Desinformação**. Publicado em Abr 2018 Disponível em https://ec.europa.eu/digital-single-market/en/code-practice-disinformation. Acesso em 12 Fev 2021.

## 2.2 PL 2630/2020 e os desafios para o combate à desinformação

Proposto em 13 de maio de 2020, pelo então Senador Alessandro Vieira, em colaboração com os então Deputados Federais Tábata Amaral e Felipe Rigoni, o projeto da "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet", conforme foi intitulado, recebeu, logo de início, muitas críticas de setores das telecomunicações, ativistas e pesquisadores do direito digital, por trazer algumas imprecisões conceituais que, na visão dos especialistas, poderiam ampliar a discricionariedade dos provedores, dando margem para o abuso de poder. Dentre os pontos mais criticados, a tentativa de definir o que seria desinformação chama atenção:

> Art. 4º Para os efeitos desta Lei, considera-se:
> [...]
> II - desinformação: conteúdo, em parte ou no todo, inequivocamente falso ou enganoso, passível de verificação, colocado fora de contexto, manipulado ou forjado, com potencial de causar danos individuais ou coletivos, ressalvado o ânimo humorístico ou de paródia[108].

Além do destaque aos conteúdos "inequivocamente falsos ou enganosos", outros pontos demonstravam a preocupação do legislador em criminalizar comportamentos comuns nas redes, por meio de medidas que se diziam inspiradas em modelos regulatórios internacionais – um meio termo entre o modelo americano e o alemão – e que, por consequência, reproduziam questões controversas tais como: a atribuição, aos provedores, da responsabilidade de rotular o conteúdo desinformativo e proceder à imediata retirada; a estipulação do dever de transparência dos provedores apenas quanto aos conteúdos patrocinados; a obrigação de identificar dos usuários por meio de documentos oficiais válidos; e, por fim, a tramitação acelerada, com pouca participação da sociedade civil, no contexto de uma crise sanitária.

Tais pontos foram alvo de diversos relatórios, notas técnicas e manifestações públicas de organizações da sociedade civil que foram significativos para que uma nova versão do projeto fosse apresentada algumas semanas após o início da tramitação. O texto substitutivo

---

[108] SENADO FEDERAL. **PL nº 2630/2020**. Proposta original protocolada em 13 Mai 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8110634&ts=1612303001672&disposition=inline. Acesso em 10 Dez 2020.

acolheu as principais críticas e incluiu outros artigos que pretendiam focar na moderação do comportamento indevido para evitar dar margem ao "policiamento discursivo" pelas plataformas, ponto tão refutado no modelo anterior.

Ocorre que, ao estipular novas modalidades de moderação, a versão substitutiva do projeto apegou-se às estratégias de monitoramento e rastreio do comportamento considerado indevido, e não mais conteúdo, como forma de preservar a liberdade de expressão, mas acabou abrindo dúvidas quanto à relativização da proteção à privacidade e da neutralidade da rede. Isso porque, após ser retirada a definição do que seria "desinformação", a nova versão do PL tratou como "conduta indevida" o envio de mensagens em massa, estipulando a guarda prévia dos dados relacionados a essas mensagens, independente do conteúdo, e o dever de identificação dos usuários como medidas para evitar a propagação de desinformação.

O texto enfrentou algumas resistências em plenário e, após sucintas modificações, foi aprovado e endereçado à Câmara dos Deputados, onde a tramitação está em curso. Ainda assim, as críticas que seguem ao modelo atual dão conta de que as medidas sugeridas estão demasiadamente apegadas ao controle repressivo, que incentiva o controle de comportamentos por sistemas automatizados, e não tanto às políticas de transparência dos intermediários, o que se revelaria incompatível com o discurso da autorregulação-regulada.

De fato, pelo menos na teoria, medidas que tenham a vigilância como fundamento denotam tudo aquilo que os modelos de corregulação pretendem desconstruir: isto é, a ideia de que o uso de sistemas preditivos pode evitar condutas indevidas, quando, em verdade, podem contribuir para moldar condutas de conformidade. No campo das liberdades de expressão, as consequências do controle preditivo para a esfera pública são inimagináveis, uma vez que pode estimular os chamados "*chilling effects*", ou seja, um efeito regressivo conduzido pelo medo de se expor. Logo, em vez de incentivar a polissemia e o dissenso, promoveria o medo e a inibição e, ainda, não resolveria o problema do controle irrestrito sobre os dados pessoais.

Ao passo que pesquisadores e especialistas seguem apontando os riscos nesta versão aprovada no Senado, do "lado de fora" do Congresso o poder judiciário e as plataformas vêm fazendo contornos para conjugar as interpretações possíveis do modelo regulatório que se firmará por aqui. No judiciário, a apreciação de casos envolvendo a propagação de "*Fake News*"

tem adotado os princípios do MCI e da LGPD como paradigmas para enfrentar os limites à privacidade e à liberdade de expressão, com tendência a determinar a retirada do conteúdo, numa evidente inspiração no modelo *Judicial and Take Down*[109]. As plataformas, por sua vez, têm publicizado medidas preventivas para monitorar o uso de *bots* e ferramentas automatizadas, e buscando se aproximar, cada vez mais, dos poderes executivo e judiciário, para pautar alternativas à responsabilização direta[110].

Mas, em que pesem os esforços empreendidos por todos os lados, fato é que o debate sobre a influência dos modelos de negócio na propagação de desinformação segue no ar. A lógica da perfilização baseada na extração irrestrita de dados pessoais sequer aparece nas pautas legislativas pesquisadas até aqui.

No mesmo sentido, a problematização da vigilância enquanto mecanismo de combate à desinformação continua sendo assunto relegado às esferas acadêmicas. Até porque, conforme destaca o pesquisador e especialista em Economia Política no cenário digital, Rafael Zanatta, abordar tais questões, no cenário legislativo principalmente, implicaria em "regulamentar e colocar limites na mercantilização dos dados pessoais", desencadeando uma série de obrigações jurídicas para os intermediários identificáveis na LGPD (2019, p. 3)[111] – o que, certamente, demandaria um espinhoso trabalho de autoanálise para o capitalismo de vigilância.

---

[109] Ver conclusões da pesquisa de CUNHA, Letícia G. **O confronto entre liberdade de expressão e *Fake News* no Brasil: uma análise dogmática e jurisprudencial**. Monografia apresentada ao curso de bacharelado em Direito. Rio de Janeiro: UFRJ, 2019, 119p. Disponível em https://pantheon.ufrj.br/bitstream/11422/12759/1/LGCunha.pdf . Acesso 10 Jan 2021.

[110] TSE. "***Google, Facebook, Twitter* e *WhatsApp* aderem ao Programa de Enfrentamento à Desinformação do TSE e Ministério da Justiça e Segurança Pública**". Notícia (online) publicada em 22 Out 2019. Disponível em ttps://www.tse.jus.br/imprensa/noticias-tse/2019/Outubro/google-facebook-twitter-e-whatsapp-aderem-ao-programa-de-enfrentamento-a-desinformacao-do-tse. Acesso em 112 Jan 2021.

[111] ZANATTA, Rafael A. F. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. In: ABRAMOVAY, Ricardo; ZANATTA, Rafael A. F. Risk regulation and data protection. (research project). Brasil: Researchgate, 2019, p. 3. Disponível em https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais. Acesso 27 Jan 2021

# 3. VIGILÂNCIA COMO MECANISMO DE COMBATE À DESINFORMAÇÃO

O cenário de alastramento da desinformação trouxe a necessidade de se discutir como as democracias devem proteger a esfera pública, cuja procedência têm se revelado mais expressivamente na esfera digital. Assim, diante da caótica discussão envolvendo redes de desinformação e uso de dados pessoais para o perfilamento do consumo na internet, nos deparamos com uma constatação menos evidente: o ciclo da desinformação está, também, atravessado pela vigilância na rede.

Mesmo que, desde 2018, algumas plataformas de mídia, como o *Facebook*, o *Instagram*, o *WhatsApp*, o *YouTube* e o *Twitter* tenham anunciado certas medidas[112] para combater a desinformação, não nos parece que elas foram pensadas para ampliar a autonomia da decisão e a diversidade informativa das pessoas, e tampouco foram discutidas com a sociedade civil e com o poder público. Aliás, conforme apontou um estudo do Intervozes (2020)[113] sobre "como as plataformas desenvolveram seus mecanismos de combate à desinformação", ficou claro que elas não buscam atender, em primazia, questões de ética ou preceitos legais. A sociabilidade humana, no seu sentido mais primitivo, é o único laboratório dessas empresas, que têm na vigilância sua metodologia de conhecimento.

A partir de então, a preocupação com a legalidade e os direitos individuais envolvidos nas dinâmicas operadas para combater a desinformação tem sido o foco dos nossos estudos. Depois disso, encontramos no PL 2630/2020, cuja tramitação já estava em processo, a oportunidade de acompanhar o debate legislativo a respeito do assunto. De lá para cá, colocamos à vista de uma estrutura metodológica mais ou menos organizada o seguinte objetivo: identificar quais direitos individuais estão em jogo no projeto de regulamentação da desinformação no Brasil, tendo como recorte de análise as medidas que sugerem mecanismos de vigilância para o enfrentamento do problema.

---

[112] Pesquisa do Intervozes mapeou as medidas adotadas pelas plataformas para o combate à desinformação no Brasil, desde 2018. Disponível em https://intervozes.org.br/publicacoes/fake-news-como-as-plataformas-enfrentam-a-desinformacao/. Acesso em 13 Fev 2021.

[113] Op. Cit. INTERVOZES, 2018.

Em princípio, nosso recorte estava endereçado na "Seção II - medidas contra a desinformação" da primeira versão do PL 2630/2020, que previa mecanismos de vigilância baseados na moderação de conteúdo. Ocorre que o PL sofreu alterações radicais durante a tramitação, sendo revestido num projeto totalmente diferente. Contudo, a previsão de medidas de vigilância permaneceu em diversos novos dispositivos. Dentre eles, o artigo 10 nos chamou mais atenção, justamente por parecer conformar o poder das plataformas sobre os dados de uma coletividade considerada "suspeita", pela definição absolutamente abstrata do que seria uma conduta condenável: o envio de uma mesma mensagem para mais de 5 usuários no período de 15 dias.

Assim, buscando empreender uma metodologia de pesquisa que se ajustasse aos nossos objetivos e, ao mesmo tempo, à dinâmica do processo legislativo, lançamos mão de um "modelo quase artesanal de ciência" – parafraseando o importante sociólogo e crítico das metodologias tradicionais da pesquisa social, Howard Becker (1993)[114] – por meio do qual chegamos a um processo analítico sobre as várias etapas da investigação, descritas a seguir.

## 3.1 Metodologia

A pesquisa no campo regulatório é um desafio, pois além de requerer constante atualização sobre as questões sociais envolvidas no propósito de uma lei, há de se ter discernimento político para interpretar como as motivações e disputas de poder se alinham no plano da eficácia e da validade da norma. Não obstante, o cenário do processo legislativo, por si só, oferece um rico material empírico aos mais distintos objetivos, métodos, áreas e interesses.

No Direito, em especial, a criação de uma lei pode ser compreendida como um fenômeno, que parte dos anseios e problemáticas de um grupo ou situação específica e, a partir do poder reservado a alguns legitimados, se transforma em um padrão aplicado a todos. Assim, alguns pesquisadores filiados à comunidade científica jurídica – que não se resume apenas aos

[114] BECKER, Howard. **Métodos de pesquisa em ciências sociais**. Tradução: Estevão Renato Aguiar. São Paulo: Editora HUCITEC, 1993, p. 12.

operadores do direito, incluindo também sociólogos, filósofos, cientistas políticas e outros – defendem que a abordagem que tenha como foco o estudo da elaboração da norma deve se debruçar, inevitavelmente, sobre o contexto fático e as circunstâncias temporais e locais que "envolvem sua justificação, alteração, aplicação e a produção de efeitos"[115]. Até porque:

> Se as leis - em sentido amplo - são a concretização de um poder de escolha do Estado para impor determinadas regras de comportamento para a sociedade, o processo pelo qual esse poder de escolha se concretiza em norma é objeto de estudo relevante para o pesquisador do direito (DE PAULA&PAIVA, 2019, p. 144).

Do mesmo modo, o estudo da criação da norma também requer uma metodologia que se adeque aos critérios e à linguagem da área na qual será debatido, visando alcançar uma discussão inteligível entre os pares que, assim como o próprio pesquisador, poderão identificar hipóteses plausíveis de validação (ou não) para a formação de novos saberes.

Assim, neste trabalho recorremos à chamada "Metodologia de Pesquisa em Direito" (QUEIROZ, 2017)[116] que, na sua complexidade, requer conhecimento e domínio dos métodos e técnicas mais adequados às questões da área, como também aptidão para lidar com a dialética das experiências sociais, com as provocações filosóficas que circundam o propósito do "dever-ser", e com a perspectiva multidisciplinar - tão própria da natureza do Direito.

Para tanto, objetivando compreender quais direitos individuais estão em jogo na elaboração do PL 2630/2020 e verificar a nossa hipótese de que alguns dispositivos foram aprovados à revelia dos direitos fundamentais, da legislação complementar especializada e do debate público qualificado, lançamos mão de um método: (i) de abordagem indutiva, para identificar "os princípios gerais e a conexão sistêmica dos institutos jurídicos" que estão em disputa na tramitação do projeto; (ii) de procedimento monográfico, que se aproxima das hipóteses de aplicação do estudo de caso, contudo tendo um dispositivo normativo (o artigo 10)

---

[115] DE PAULA, Felipe; PAIVA, Luiz Guilherme M de. **A pesquisa legislativa: fontes, cautelas e alternativas à abordagem tradicional**. In: QUEIROZ, Rafael Maffei R.; FEFERBAUM, Marina (Coord.). Metodologia da pesquisa em direito: técnicas e abordagens para elaboração de monografias, dissertações e teses. 2ª Edição. São Paulo : Saraiva, 2019, p. 138-163.

[116] QUEIROZ, Rafael Mafei R. **Metodologia da pesquisa jurídica**. In: CAMPILONGO, Celso F,; GONZAGA, Alvaro de A.; FREIRE, André Luiz(coords.). Enciclopédia jurídica da PUC-SP. 1ª Edição. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em https://enciclopediajuridica.pucsp.br/verbete/151/edicao-1/metodologia-da-pesquisa-juridica. Acesso em 12 Fev 2021.

como recorte de análise para se pensar os impactos das medidas de rastreabilidade decorrentes dele; (iii) de interpretação sistemática, para tentar visualizar as possibilidades de harmonia com os demais instrumentos normativos hierarquicamente superiores ou entendimentos doutrinários afins.

A tipologia da presente pesquisa pode ainda ser classificada como teórica, quanto a sua natureza, e analítica quanto aos objetivos, na medida em que pretende analisar o texto legislativo do PL, mais especificamente o do artigo 10, a partir do embasamento conceitual sobre desinformação, vigilância e proteção de dados. Quanto aos procedimentos da tipologia, utilizou-se a pesquisa bibliográfica para o levantamento de referências teóricas e doutrinárias; e também a pesquisa documental, para localizar os textos legislativos, pedidos de emendas e notas técnicas pertinentes ao assunto. No que tange especificamente ao objeto estudado, qual seja o PL 2630/2020, realizamos uma pesquisa legislativa, tendo como foco a tramitação da versão aprovada no Senado (Casa de origem) em 30 de junho de 2020 e encaminhada à Câmara dos Deputados (Casa revisora) em 03 de julho de 2020, e que até a conclusão deste trabalho aguardava a votação nesta última.

Assim, para melhor interpretarmos as mudanças realizadas no projeto, acompanhamos a tramitação no Senado e na Câmara dos Deputados – entre 15 de maio de 2020 a 03 de julho de 2020 – por meio do serviço de *push*[117], além de verificarmos todos os relatórios e notas técnicas apresentadas, pelas organizações da sociedade civil, a ambas as casas legislativas até a data de 19 de janeiro de 2021.

Desde a propositura, no Senado, o projeto recebeu 7 (sete) pedidos de retirada de pauta; 1 (um) pedido de adiamento para apreciação da Comissão de Constituição, Justiça e Cidadania (CCJC); e 152 pedidos de Emenda pelos gabinetes dos Senadores, dentre as quais dois assuntos foram votados em separado: 20 (vinte) Emendas[118], que propunham a reelaboração ou a

[117] O serviço de *push* é um tipo de tecnologia utilizada para a notificação de atualizações e distribuição de informação contínua sobre processos judiciais, legislativos e administrativos. Assim, toda vez que há qualquer movimentação no curso do processo em determinado órgão ou instituição, o sistema dispara um e-mail de notificação aos usuários cadastrados.

[118] Do total de 152 Emendas, aquelas que tinham como objeto de discussão o artigo 10 foram: Emenda 05 (Senadora Rose de Freitas); Emenda 08 (Senador Paulo Paim); Emenda 12 (Senadora Rose de Freitas); Emenda 13 (Senador Antônio Anastasia); Emenda 27 (Senadora Eliziane Gama); Emenda 28 (Senador Vanderlan Cardoso); Emenda 55(Senador Alessandro Vieira); Emenda 65 (Senadora Eliziane Gama); Emenda 75 (Senador Humberto Costa); Emenda 85 (Senador Rodrigo Cunha); Emenda 86 (Senador Paulo Paim); Emenda 89 (Senador

supressão do artigo 10; e a Emenda 142, que requereu a supressão do artigo 7º por entender abusiva e perigosa a obrigatoriedade de identificação, mediante apresentação de documento civil válido, dos usuários de aplicativos e redes sociais como medida preventiva à desinformação. No resultado final, o conjunto de Emendas para a reelaboração do artigo 10 foi aprovado por 40 votos (sim) votos a 32 (não), sem abstenção, nos termos da proposta encaminhada pelo Senador Rogério Carvalho (Emenda 46) e conforme relatório consignado pelo relator, então presidente da Comissão das *Fake News*[119], Senador Ângelo Coronel, que foi o responsável pela versão final do projeto aprovado[120]. A Emenda 142, todavia, foi reprovada por 41 votos (não) a 28 (sim), com uma abstenção.

Após aprovada a versão substitutiva do projeto (versão atual) em 30 de junho de 2020, representantes de entidades do setor das telecomunicações[121], institutos de pesquisas e

Wellington Fagundes); Emenda 91 (Senador Weverton); Emenda 92 (Senador Esperidião Amin); Emenda 95 (Senador Luiz do Carmo); Emenda 117 (Senador Eduardo Gomes); Emenda 126 (Senadora Daniella Ribeiro); Emenda 137 (Senador Randolfe Rodrigues); Emenda 140 (Senador Randolfe Rodrigues); Emenda 146 (Senador Rogério Carvalho). **Coleta e triagem realizadas pela autora**. Informações disponíveis em https://www25.senado.leg.br/web/atividade/materias/-/materia/141944#emendas. Acesso 27 Jan 2021.

[119] A Comissão Parlamentar Mista de Inquérito das *Fake News* foi instaurada em setembro de 2019 para "Investigar, no prazo de 180 dias, os ataques cibernéticos que atentam contra a democracia e o debate público; a utilização de perfis falsos para influenciar os resultados das eleições 2018; a prática de *cyberbullying* sobre os usuários mais vulneráveis da rede de computadores, bem como sobre agentes públicos; e o aliciamento e orientação de crianças para o cometimento de crimes de ódio e suicídio". Informações a respeito dos trabalhos, agenda e composição da comissão estão disponíveis em https://legis.senado.leg.br/comissoes/comissao?8&codcol=2292. Acesso em 30 Jan 2021.

[120] Relatório final, com a versão aprovada, considerando as Emendas acatadas e rejeitadas, disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8127630&ts=1612303014059&disposition=inline . Acesso em 27 Jan 2021.

[121] (i) Ofício n° 034 de 2020, da Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - FEDERAÇÃO ASSESPRO, remetido ao Senado em 25 de junho de 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8869048&ts=1612303018235&disposition=inline. Acesso em 27 Jan 2021.
(ii) Oficio nº 041 de 2020, da Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - FEDERAÇÃO ASSESPRO, remetido ao Senado em 30 de junho de 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8920333&ts=1612303018626&disposition=inline. Acesso em 27 Jan de 2021.

associações com atuação na área da tecnologia[122], conselhos de área[123], e uma Câmara Municipal[124], apresentaram ofícios, notas técnicas e manifestações no sentido de alertar os parlamentares para os perigos relacionados à violação de direitos fundamentais, excesso de vigilância e imprecisões técnicas no projeto. Assim, pugnaram pela "realização de um conjunto de audiências públicas, seminários e fóruns que permitam a interlocução com a sociedade e o amadurecimento da proposta apresentada"[125]. Contudo, a tramitação seguiu seu curso e o projeto foi encaminhado para votação na Câmara dos Deputados.

Na Câmara dos Deputados, por sua vez, o projeto recebeu 7 (sete) pedidos de apenso[126] para tramitação conjunta com outros projetos de mesma temática, que estavam "travados" nas Comissões Especiais. Como o projeto substitutivo já havia sido aprovado no plenário do Senado, haveria então a obrigatoriedade de que a discussão na Câmara (Casa revisora) também se desse no plenário. Assim, os pedidos de apenso significam uma oportunidade para que os projetos até então parados nas Comissões Especiais pudessem "pular a etapa" da admissibilidade e serem discutidos, ainda que pontualmente, no plenário da Câmara.

Esta, no entanto, não parece ter sido a única estratégia em curso para a sobreposição de pautas que fossem melhor recepcionadas na regulamentação das *Fake News*. Cabe lembrar que

---

[122] (i) Nota técnica da Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação - BRASSCOM, apresentada ao Senado em 24 de junho de 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8869040&ts=1612303018361&disposition=inline. Acesso em 27 Jan 2021.
(ii) Manifestação da Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação - Brasscom, apresentada ao Senado em 25 de junho de 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8868992&ts=1612303018273&disposition=inline. Acesso em 27 Jan 2021.
(iii) Manifestação da Câmara Brasileira de Comércio Eletrônico (CÂMARA-E.NET), apresentada ao Senado em 19 de janeiro de 2021. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8920339&ts=1612303018584&disposition=inline. Acesso em 27 Jan 2021.

[123] (i) Parecer do Conselho Empresarial Brasil-Estados Unidos da U.S. Chamber of Commerce, apresentado ao Senado em 25 de junho de 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8869022&ts=1612303018314&disposition=inline. Acesso em 27 Jan 2021.
(ii) OAB, Conselho Federal. Processo n. 49.0000.2020.00438-0 que trata da Proposição, pelo Conselho Federal da Classe, de parecer legislativo sobre o PL nº 2630/2020. Debatido no plenário do Conselho Federal em 07 de julho de 2020. Brasília: OAB, 2020, p.1-26. Disponível em https://www.conjur.com.br/dl/fragil-vago-projeto-fake-news-oab.pdf. Acesso em 09 Fev 2021.

[124] Ofício nº PR/DL 107/2020, da Câmara Municipal de Jundiaí (SP), remetido ao Senado em 02 de junho de 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8920337&ts=1612303018668&disposition=inline . Acesso em 27 Jan de 2021.

[125] Op. Cit. BRASSCOM, 2020, p.3.

[126] Neste trabalho, foram considerados todos os pedidos de apenso apresentados pelos Deputados até 19 de janeiro de 2021. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_requerimentos?idProposicao=2256735. Acesso em 20 Jan 2021.

antes de o PL 2630/2020 ser aprovado em primeiro turno no Senado, outros quatro projetos, de conteúdos similares, já haviam sido apresentados na Câmara e no Senado, respectivamente. Trata-se do PL 1429/2020[127], proposto em 1º de abril de 2020 na Câmara dos Deputados; o PL 1358/2020[128], proposto em 2 de abril de 2020 no Senado; o PL 2927/2020[129], proposto em 26 de maio de 2020 na Câmara e o PL 3063/2020[130], proposto em 2 de junho de 2020 também na Câmara dos Deputados.

As três primeiras propostas foram retiradas de pauta, a pedido de seus autores – que, por sinal, foram os mesmos em todas elas – após uma série de inconsistências sobre os conceitos de "desinformação", "impulsionamento", "patrocínio", "provedores de aplicação", entre outros, serem apontadas por institutos com atuação e pesquisa em tecnologia[131] e também após receberem expressiva avaliação negativa nas consultas públicas promovidas pelas casas legislativas[132].

O único que ainda aguarda admissibilidade na Câmara é o PL 3063/2020, que, mesmo após a tramitação do PL 2630/2020, foi mantido em pauta por seus autores sob a justificativa de que não possui o mesmo conteúdo das demais versões apresentadas. Segundo defendem, diferente das versões anteriores, o PL 3063/2020 estaria "alinhado com o Marco Civil da

---

127 CÂMARA DOS DEPUTADOS. PL 1429/2020. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242713 . Acesso em 21 Jan 2021.

128 SENADO FEDERAL. PL 1358/2020. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/141372. Acesso em 21 Jan 2021.

129 CÂMARA DOS DEPUTADOS. PL 2927/2020. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2253807. Acesso em 21 Jan 2021.

130 CÂMARA DOS DEPUTADOS.PL 3063/2020. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2254270. Acesso em 21 Jan 2021.

131 (i) COALIZÃO DIREITOS NA REDE. Nota pública sobre os PL 1429/2020 e 2630/2020. Disponível em https://www.codingrights.org/nota-publica-sobre-o-projeto-da-lei-brasileira-de-liberdade-responsabilidade-e-transparencia-na-internet-pl-1429-2020-e-pl-2630-2020/ . Acesso em 21 Jan 2021.
(ii) CODING RIGHTS e IP.REC. Nota técnica sobre os PL 1429/2020 e PL 1358/2020. Disponível em https://www.codingrights.org/nota-nota-tecnica-sobre-pl-1429-2020-e-pl-1358-2020-que-instituem-a-lei-brasileira-de-liberdade-responsabilidade-e-transparencia-na-internet/. Acesso em 21 Jan 2021.
(iii) INTERVOZES. Nota técnica sobre os PL 1429/2020 e PLS 1358/2020. Disponível em https://intervozes.org.br/publicacoes/nota-tecnica-sobre-plc-desinformacao-2020/. Acesso em 21 Jan 2021.
(iv) LAPIN. Nota Técnica sobre o PL 1429/20. Disponível em https://lapin.org.br/wp-content/uploads/2020/08/NT_PL_1429_-_Desinformacao.pdf. Acesso em 21 Jan 2021.

132 (i) CÂMARA DOS DEPUTADOS. Consulta pública do PL 1420/20. Disponível em https://forms.camara.leg.br/ex/enquetes/2242713/resultado .Acesso em 21 Jan 2021.
(ii) SENADO FEDERAL. Consulta pública do PL 1358. Disponível em https://www12.senado.leg.br/ecidadania/visualizacaomateria?id=141372.Acesso em 21 Jan 2021.
(iii) CÂMARA DOS DEPUTADOS. Consulta pública do PL 2927/20. Disponível em https://forms.camara.leg.br/ex/enquetes/2253807/resultado. Acesso em 21 Jan 2021.

Internet" e não ofereceria "riscos à privacidade dos usuários", tendo como focos prioritários as "políticas de transparência e o combate aos robôs não identificados"[133].

Até o fechamento da coleta de dados para este trabalho, tanto o PL 2630/2020 quanto o PL 3063/2020 aguardavam deliberação da Mesa Diretora da Câmara para irem ao plenário. O PL 2630/2020, porém, já está com o processo mais avançado e, caso seja aprovado sem modificações, segue para sanção ou veto do Presidente da República.

Como bem se vê, não foram poucas as tratativas de parlamentares em minoria, representantes da sociedade civil e instituições de pesquisa em demonstrar que as propostas de regulamentação da desinformação têm muitos pontos controversos e que ainda carecem de debates mais amplos, qualificados e plurais.

Em especial no PL 2630/2020, observou-se que, durante toda a tramitação, a preocupação com a privacidade e com a proteção de dados movimentou as discussões em torno das medidas específicas para conter a desinformação, numa visível disputa pela possibilidade de implementar mecanismos de vigilância por meio da identificação e do armazenamento dos dados com vistas à repreensão de comportamentos inautênticos - conceito que, aliás, não é claramente definido em nenhum dos projetos apresentados.

Diante desse cenário, optamos por delimitar a nossa discussão àquela medida que, aos olhares mais desavisados, soa como um mecanismo eficaz para o combate não apenas à desinformação como a ações de criminalidade cibernética derivadas: o artigo 10, que trata do dever de guarda, pelos provedores intermediários, dos dados referentes aos envios de mensagens em massa.

Sem embargo, ainda que a proposta do artigo 10 pareça atender tanto os discursos mais punitivistas, que incentivam a definição e coerção de "tipos comportamentais inautênticos", quanto aqueles mais progressistas, que vêem no dispositivo uma alternativa ainda em construção, fato é que essa "solução" não pode ser legitimada em desarmonia com as garantias

[133] Um dos autores publicou, em sua página pública no *Facebook*, a justificativa para manter o PL 3063/2020 em pauta mesmo após a aprovação do PL 2630/2020 no Senado. Disponível em https://www.facebook.com/tabataamaralSP/posts/696957764192831/. Acesso em 21 Jan 2021.

constitucionais, com a legislação especial, com as referências internacionais que já disciplinam a matéria, e, por fim, à revelia das manifestações da sociedade civil.

E, para entendermos no que consistem tais controvérsias, discutiremos a redação até então aprovada e quais direitos e garantias são abrangidos pelos procedimentos previstos no *caput* e incisos.

## 3.2 O registro da cadeia de encaminhamentos e o fator da rastreabilidade

Antes de adentrarmos na questão da rastreabilidade enquanto medida de vigilância, é necessário fazer uma retomada das discussões que levaram à redação atual do artigo 10. O projeto original previa um capítulo para a responsabilização “dos provedores de aplicação no combate à desinformação e no aumento da transparência na internet” (Capítulo II), que foi mantido, porém com a alteração da redação para “responsabilidade no uso de redes sociais e de serviços de mensageria privada”. A estrutura inicial do capítulo continha quatro seções, que tratavam de disposições gerais (Seção I); dever de transparência dos provedores de aplicação (Seção II); medidas contra a desinformação (Seção III) e serviços de mensageria privada (Seção IV).

Contudo, no projeto aprovado, a seção que tratava do dever de transparência dos intermediários foi renomeada para "Cadastro de contas" (Seção II), que dispõe sobre a possibilidade de os provedores de redes sociais e de mensagem exigirem a identificação dos usuários, com documento de identidade oficial, para o uso do serviço. Já a seção que tratava das "medidas contra a desinformação" foi absorvida pelos deveres "dos serviços de mensageria privada" (Seção III), ou seja, ela deixou de existir enquanto parte destacada no projeto, para dar lugar à Seção que trata dos "procedimentos de moderação" de conteúdos (Seção IV).

Neste ponto, importa destacar que as medidas de combate à desinformação previstas no projeto original se confundiam com os procedimentos de moderação de conteúdo, e foram bastante criticadas pelos próprios Senadores em plenário, por conferirem demasiado poder aos

provedores dos serviços para decidir sobre a veiculação e retirada de publicações consideradas inadequadas. Sobretudo o artigo 10, que estipulava ações para a identificação e interrupção dos serviços, não esclareceu quais seriam os critérios utilizados para o que chamou de "verificações provenientes dos verificadores de fatos independentes com ênfase nos fatos" e, tampouco, previa a chance de contraditório às contas suspeitas. Somente após a remoção e notificação de todas as contas e usuários que compartilharam o conteúdo considerado fraudulento, é que haveria a possibilidade de retratação, conforme assinalou o artigo 11.

> Seção III
> Das Medidas contra a Desinformação
>
> Art. 9º Aos provedores de aplicação de que trata esta Lei, cabe a tomada de medidas necessárias para proteger a sociedade contra a disseminação de desinformação por meio de seus serviços, informando-as conforme o disposto nos artigos 6º e 7º desta Lei.
> Parágrafo único. As medidas estabelecidas no *caput* devem ser proporcionais, não discriminatórias e não implicarão em restrição ao livre desenvolvimento da personalidade individual, à manifestação artística, intelectual, de conteúdo satírico, religioso, ficcional, literário ou qualquer outra forma de manifestação cultural.
> **Art. 10. Consideram-se boas práticas para proteção da sociedade contra a desinformação:**
> **I – o uso de verificações provenientes dos verificadores de fatos independentes com ênfase nos fatos;**
> **II – desabilitar os recursos de transmissão do conteúdo desinformativo para mais de um usuário por vez, quando aplicável;**
> **III – rotular o conteúdo desinformativo como tal;**
> **IV – interromper imediatamente a promoção paga ou a promoção gratuita artificial do conteúdo, seja por mecanismo de recomendação ou outros mecanismos de ampliação de alcance do conteúdo na plataforma.**
> **V – assegurar o envio da informação verificada a todos os usuários alcançados pelo conteúdo desde sua publicação.**
> Art. 11. Caso o conteúdo seja conside, os provedores de aplicação devem prestar esclarecimentos ao primeiro usuário a publicar tal conteúdo, bem como toda e qualquer pessoa que tenha compartilhado o conteúdo, acerca da medida tomada, mediante exposição dos motivos e detalhamento das fontes usadas na verificação.
> Art. 12. Os provedores de aplicação devem fornecer um mecanismo acessível e em destaque, disponível por no mínimo três meses após a decisão, para que o usuário criador ou compartilhador do conteúdo, bem como o usuário autor de eventual denúncia possa recorrer da decisão.
> §1º Deve ser facultada ao usuário a apresentação de informação adicional a ser considerada no momento da revisão.
> §2º Caso a revisão seja considerada procedente pelo provedor de aplicação, este deve atuar para reverter os efeitos da decisão original.
> (Grifos nossos)

De fato, no contexto em que foi inserido, o comando do artigo 10 previa medidas muito imediatas, que visavam conter o problema na fonte, porém eram evasivas de sentido na prática. Isso porque desconsideravam que o alastramento da desinformação na internet é um fenômeno,

ou seja, algo que vai se transformando dentro de seus próprios efeitos; não partindo apenas de uma fonte, em apenas uma plataforma ou rede social, nem sempre é intencional, e, muitas vezes, sendo impossível identificar onde surgiu.

Logo, por não apresentar uma solução consistente para o propósito maior do projeto, qual seja, evitar e punir a propagação de desinformação, a redação original foi suprimida e, no seu lugar, foram readequadas as propostas antes inseridas no artigo 13, que trazia definições e restrições aos "encaminhamentos em massa" no contexto eleitoral.

> Art. 13. Os provedores de aplicação que prestarem serviços de mensageria privada desenvolverão políticas de uso que limitem o número de encaminhamentos de **uma mesma mensagem a no máximo 5 (cinco) usuários ou grupos**, bem como o número máximo de membros de cada grupo de usuários para o máximo de 256 (duzentos e cinquenta e seis) membros.
> §1º **Em período de propaganda eleitoral**, estabelecido pelo art. 36 da Lei 9.504 de 1997 e durante situações de emergência ou de calamidade pública, **o número de encaminhamentos de uma mesma mensagem fica limitado a no máximo 1 (um) usuários ou grupos**. (Redação do projeto original, grifos nossos)

No projeto aprovado, a ideia do artigo 13 foi quase que integralmente utilizada na nova redação do artigo 10[134], porém estendendo a cogência da norma ao contexto geral e não apenas ao período de eleições. Além disso, aproveitou-se o prazo de três meses para a guarda dos registros dos encaminhamentos considerados suspeitos, antes previsto no artigo 12, acrescentando-se o dever de identificação de todos os usuários afetados pela cadeia de encaminhamentos com o objetivo de facilitar eventual investigação criminal:

> **Art. 10. Os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses, resguardada a privacidade do conteúdo das mensagens.**
>
> § 1º Considera-se encaminhamento em massa do envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 (quinze) dias, para grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários.
>
> § 2º Os registros de que trata o caput devem conter a indicação dos usuários que realizaram encaminhamentos em massa da mensagem, com data e horário do encaminhamento e o quantitativo total de usuários que receberam a mensagem.

[134] SENADO FEDERAL. **PL nº 2630/2020**. Texto substitutivo aprovado em 30 Jun 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8128670&ts=1612303015028&disposition=inline. Acesso em 10 Dez 2020.

> § 3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento em massa de conteúdo ilícito, para constituição de prova em investigação criminal e em instrução processual penal, mediante ordem judicial, nos termos da Seção IV do Capítulo II da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
>
> § 4º A obrigatoriedade de guarda prevista neste artigo não se aplica às mensagens que alcançarem quantitativo total inferior a 1.000 (mil) usuários, devendo seus registros ser destruídos nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

Conforme já sinalizado na seção anterior, mesmo o conteúdo previsto nesta redação substitutiva foi objeto de questionamento por Senadores que propuseram as Emendas 95, 126, 137 e 140, alegando que o dispositivo poderia: (i) instituir um "mecanismo de rastreabilidade do fluxo de mensagens"; (ii) violar as garantias constitucionais de sigilo das comunicações pessoais e a presunção de inocência; (iii) além de não especificar a quais plataformas estaria designado o dever de guarda e registro, já que a expressão "serviços de mensageria privada" é demasiadamente abrangente, compreendendo desde redes sociais, aplicativos de mensagens (como *WhatsApp, Telegram, Signal, Clubhouse*, entre outros) até mesmo os serviços de *E-mail*.

Importante frisar que tais Emendas tiveram por base a opinião técnica de organizações da Sociedade Civil e pesquisadores universitários[135] que questionavam, entre outros pontos, em quais estudos ou evidências estaria baseada a ideia que o armazenamento preditivo da cadeia de encaminhamentos em massa poderia diminuir a incidência de desinformação. Segundo destacam as notas técnicas, seria praticamente impossível identificar a autoria de um conteúdo falso, considerando que muitas vezes as postagens são replicadas, em diferentes formatos (textos, memes, *prints*, imagens, vídeos, *hashtags*), de uma plataforma a outra.

Além disso, lembram que diferente de como ocorre quando se mantém registros telefônicos ou de conexão, a manutenção de toda a cadeia de encaminhamento implicaria em registrar a movimentação comunicativa de vários usuários vinculados a determinada

[135] Dentre as Organizações citadas nas Emendas aparecem a Coalização de Direitos na Rede; a *Coding Rights* e a *Data Privacy Brasil*. Outras organizações também contribuíram com o debate técnico. A lista completa está disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8869040&ts=1612303018361&disposition=inline . Acesso em 21 Jan 2021. Dentre os pesquisadores mencionados nas Emendas aparecem os Dres. Ricardo Campos e Juliano Maranhão. Optamos por não nomear quais Senadores se respaldaram nessas opiniões técnicas porque entendemos que o intuito deste trabalho não é personalizar o mérito de ações que, em verdade, fazem parte das obrigações parlamentares.

mensagem, e não apenas nome, data e horário de envio. Isso significa, por exemplo, que se um usuário encaminhar uma mensagem para 10 grupos de 100 pessoas no *WhatsApp*, e cada uma dessas pessoas compartilhar a mensagem para outros grupos, num intervalo de 15 dias conforme prevê o projeto, as plataformas repetiriam a operação de armazenar os dados vinculados àquela cadeia inicial pelo menos mil vezes. Ou seja, além de desproporcional, seria contraproducente até mesmo para os próprios modelos de negócio e ainda haveria dúvidas sobre quem, de fato, foi o autor da corrente de desinformação.

Outro ponto interessante sinalizado nas notas técnicas é o fato de que para as quadrilhas especializadas na disseminação de conteúdo falso seria relativamente "fácil" burlar um sistema de armazenamento preditivo que tenha como único gatilho "o envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 dias". A esse respeito, a nota da organização *Data Privacy* Brasil traz um trecho elucidativo:

> Ao criar um sistema rígido ou uma padronização para a rastreabilidade de mensagens, é provável que isso abra a oportunidade de técnicas para "enganar o sistema" (*game the system*). [...] Seria fácil, por exemplo, automatizar um *script* para que um mesmo texto desinformador fosse editado de inúmeras formas distintas, por meio de pequenas modificações em número de caracteres, uso de vírgulas e pontuação ou mesmo substituição de palavras sinônimas. Neste caso, abriria-se uma situação peculiar. Uma empresa de "estratégia digital" especializada em disparos de mensagens por Whatsapp poderia utilizar uma equipe de programadores para desenvolver uma solução deste tipo – algo que pudesse enganar o sistema e evitar a rastreabilidade –, ao passo que todas as pessoas comuns, que repassam mensagens por motivações políticas espontâneas, teriam os dados pessoais coletados (DATA PRIVACY BRASIL, 2020, p. 10)[136].

Apesar de todos os riscos apontados, as notas técnicas também sugeriram alternativas, que envolvem aumentar o incentivo ao código de boas condutas nas redes; evitar repassar o poder de sanção às plataformas; cobrar a neutralidade tecnológica no tratamento de dados e na definição algorítmica dos modelos de negócio; e reforçar o entendimento, já previsto no Marco Civil da Internet, de que a imposição de medidas restritivas ao sigilo das comunicações é procedimento *a posteriori* e só poderia ser demandada pelas autoridades policiais, em caso de investigação, ou judiciárias, em caso de sanção.

---

[136] DATA PRIVACY BRASIL. Rastreabilidade, metadados e Direitos Fundamentais: nota técnica sobre o projeto de Lei 2630/2020. Disponível em https://www.dataprivacybr.org/wp-content/uploads/2020/07/Data-Privacy-Brasil.-Rastreabilidade-e-Direitos-Fundamentais.-PL-2630.2020.pdf. Acesso em 27 Jan 2021.

Em contrapartida, os argumentos das notas técnicas foram preteridos no plenário em relação às propostas de Emendas a favor do artigo 10, que revelaram o intuito de manter o armazenamento dos envios em massa como critério de verificação das condutas inautênticas e, portanto, fundamento para a pretensão punitiva desse comportamento.

No parecer final, que acolheu as teses a favor do artigo, o relator do projeto defendeu que a determinação de armazenamento estaria restrita aos dados de envio, não atingindo o conteúdo das mensagens. Além disso, ponderou que ainda que um indivíduo "manipulado" tenha repassado uma mensagem cuja rede de encaminhamentos foi considerada inautêntica, o dever de guarda só abrangeria os dados do envio daquela mensagem, e não das demais atividades do indivíduo. Portanto, não haveria que se falar em violação da privacidade e tampouco de rastreabilidade.

Do lado de fora do plenário, um terceiro argumento ganhou o respaldo de alguns especialistas em direito digital[137], que se colocam a favor do prazo para o armazenamento dos dados. Eles defendem que em comparação ao Marco Civil, o tempo de 3 (três) meses para guarda dos dados foi razoável, tendo em vista que no artigo 15 daquela Lei há a previsão de armazenamento pelos provedores de conexão por até 6 (seis) meses, tempo que ainda pode ser aumentado mediante ordem judicial. Além disso, ressaltam que outras leis preveem tal obrigação, por tempo equivalente ou até maior, como é o caso da Lei de Lavagem de Dinheiro (Lei nº 9.613/1998) e a Lei de Organizações Criminosas (Lei nº 12.850/2013). Assim, acreditam que falar em "rastreabilidade" seja um exagero, mas se usado, o mais correto seria a "rastreabilidade de comportamento", que é um dos espíritos do projeto (ABRUSIO *et al*, 2020)[138].

De fato, na votação, prevaleceram as opiniões a favor da redação atual. Mas ainda que os argumentos prós e contras tenham elucidado toda ambiguidade do dispositivo, importa ainda colocarmos algumas considerações que não apareceram no debate legislativo formal.

---

[137] Uma boa síntese dos argumentos a favor do artigo 10 está no artigo publicado por ABRUSIO et al. **Vigilância em massa ou combate à desinformação: o dilema do rastreamento**. Revista Consultor Jurídico. Coluna Direito Digital. Publicado em 04 Ago 2020. Disponível em https://www.conjur.com.br/2020-ago-04/direito-digital-dilema-rastreamento-pl-fake-news. Acesso em 10 Jan 2021.

[138] Op. cit. ABRUSIO et al., 2020.

A primeira delas consiste em apontar a fragilidade do argumento de que o dever de armazenamento só abrangeria os dados de envio, e por isso não afetaria a privacidade das pessoas. Essa afirmação apresenta um problema de inversão lógica do legislador, possivelmente intencional, porque coloca o dever de retenção dos dados antes da verificação de autenticidade da conduta. Ou seja, da forma como o artigo está estruturado, primeiro se armazenaria os dados de qualquer envio em massa para, depois, avaliar se o conteúdo é desinformação ou não.

A segunda consideração está na falácia de que o "espírito do projeto" seja combater o comportamento inautêntico e não o conteúdo das comunicações. Ora, se o próprio dispositivo justifica o armazenamento de dados em massa pela possibilidade de encontrar a autoria dos conteúdos fraudulentos na cadeia de encaminhamento, logo, é a cadeia de encaminhamento que vincula um indivíduo ao conteúdo – a mesma lógica anterior – e isso inclui armazenar muito mais dados do que apenas nome, data de envio e destinatário.

Um usuário pode ter seus dados envolvidos em mais de uma cadeia de encaminhamento e, a partir disso, é possível saber o tipo de conteúdo que produz e consome; com quem ele interage; quais dias; horários; plataformas etc. Daí porque não se pode comparar o registro de uma "cadeia de encaminhamentos" com os registros telefônicos previstos na Lei das Organizações Criminosas (artigo 17 da Lei nº 12.850/2013) ou com registros de conexão (IP) previstos no Marco Civil da Internet (artigos 13 e 15 da Lei nº 12.965/2014), porque nenhum deles vincula os usuários diretamente ao conteúdo das mensagens e tampouco permitem inferir sobre os hábitos de suas vidas privadas.

Apenas a título de exemplo, na seara penal, o STJ já enfrentou diversas vezes a controvérsia a respeito da ilicitude de provas obtidas por meio de registros do *WhatsApp*, sem autorização judicial, tanto em casos de flagrante delito quanto em investigações sobre tráfico de drogas e associações criminosas. Em todas elas, o que se tem afirmado, desde o consenso formado nos Informativos nº 583 e 593, é que "sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no *whatsapp* presentes no celular do suposto autor de fato delituoso". Isso porque, o que se pretende preservar é a inviolabilidade da intimidade e da vida privada pelo sigilo telefônico e das comunicações, que não se confundem com a interceptação telefônica, que é medida

excepcional precedida por autorização judicial devidamente motivada. A esse respeito, vejamos o reiterado julgado do HC nº 89.981/MG/2017:

> PENAL E PROCESSO PENAL. RECURSO EM HABEAS CORPUS. FURTO E QUADRILHA. APARELHO TELEFÔNICO APREENDIDO. VISTORIA REALIZADA PELA POLÍCIA MILITAR SEM AUTORIZAÇÃO JUDICIAL OU DO PRÓPRIO INVESTIGADO. VERIFICAÇÃO DE MENSAGENS ARQUIVADAS. VIOLAÇÃO DA INTIMIDADE. PROVA ILÍCITA. ART. 157 DO CPP. RECURSO EM HABEAS CORPUS PROVIDO. 1. Embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação telefônica, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no art. 5º, inciso XII, da CF, houve sim violação dos dados armazenados no celular do recorrente (mensagens de texto arquivadas - *WhatsApp*). **2. No caso, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista a garantia, igualmente constitucional, à inviolabilidade da intimidade e da vida privada, prevista no art. 5º, inciso X, da CF. Dessa forma, a análise dos dados telefônicos constante dos aparelhos dos investigados, sem sua prévia autorização ou de prévia autorização judicial devidamente motivada, revela a ilicitude da prova, nos termos do art. 157 do CPP. Precedentes do STJ.** 3. Recurso em habeas corpus provido, para reconhecer a ilicitude da colheita de dados do aparelho telefônico dos investigados, sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos. (Grifos nossos. STJ, 5ª Turma, RHC nº 89.981/MG, Rel. Ministro Reynaldo Soares da Fonseca, julgado em 13/12/2017)[139].

O mesmo raciocínio recentemente foi aplicado aos casos de obtenção de provas por meio do espelhamento de conversas do *WhatsApp* em navegadores, a partir dos quais entendeu a relatora, Ministra Laurita Vaz, que a obtenção de registros de conversas telefônicas por espelhamento "equivaleria a 'um tipo híbrido de obtenção de prova', um misto de interceptação telefônica (quanto às conversas futuras) e de quebra de sigilo de e-mail (quanto às conversas passadas), para os quais, pelo menos por agora, não há previsão legal" (Informativo 640 do STJ)[140].

Outro entendimento recente envolvendo a quebra de sigilo de dados informáticos em massa foi a polêmica decisão da 3ª Turma do STJ no caso das investigações da morte da vereadora Marielle Franco, ocorrida em 2018. Na discussão, ainda em primeira instância, foi determinado à empresa *Google* Brasil a entrega dos dados, como IPs e Device IDs, de todos os

---

139 STJ, 5ª Turma, RHC nº 89.981/MG, Rel. Ministro Reynaldo Soares da Fonseca, julgado em 13/12/2017. Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1663002&num_registro=201702509663&data=20171213&formato=PDF. Acesso em 08 Fev 2021.

140 STJ. 6ª Turma. RHC 99.735-SC, Rel. Min. Laurita Vaz, julgado em 27/11/2018. Disponível em https://scon.stj.jus.br/docs_internet/informativos/PDF/Inf0640.pdf. Acesso em 08 Fev 2021.

usuários que pesquisaram palavras-chaves relacionadas ao crime durante a noite do ocorrido e em áreas delimitadas pelas investigações. O requerimento, realizado pelo Ministério Público e pela Polícia Civil do Rio de Janeiro, baseou-se na indispensabilidade da medida para a solução do caso. A *Google* recorreu, alegando que não haveria embasamento legal para tal medida, que se mostrava desproporcional frente aos riscos à privacidade de centenas de usuários.

No STJ, todavia, prevaleceu o entendimento de que o acesso aos dados pessoais em massa coletados por provedores pode se dar por determinação judicial para fins de auxiliar as investigações criminais, e sua determinação impõe a apresentação dos requisitos previstos nos artigos 22 e 23 do MCI, quais sejam: (i) indícios da ocorrência do ilícito; (ii) justificativa da utilidade da requisição; e (ii) período ao qual se referem os registros. Quanto à proporcionalidade de medidas como essa, destacou o relator do caso:

> RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. IDENTIFICAÇÃO DE USUÁRIOS EM DETERMINADA LOCALIZAÇÃO GEOGRÁFICA. IMPOSIÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OCORRÊNCIA. PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO. 1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. **No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital**. 2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. **De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.** [...] 10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, **é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam – tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional – não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato**

> **investigado, serão descartados** 11. Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes cometidos por agentes públicos contra as vidas de três pessoas - mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura estatal fluminense - não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada. 12. Recurso em mandado de segurança não provido. (Grifos nossos. STJ, 3ª Turma. RMS nº 62.143/RJ. Rel. Ministro Rogério Schietti Cruz, julgado em 26/08/2020)[141].

Ou seja, mesmo nas hipóteses em que a jurisprudência entende ser proporcional a quebra do sigilo de registros informáticos em massa, há a reserva de jurisdição como mecanismo precedente.

Com efeito, a despeito de eventuais dúvidas sobre quais dados estão abrangidos pela expressão "registro", sustentamos que os registros referidos no artigo 10 do PL 2630/2020 não se resumem aos "dados de conexão", assim previstos no artigo 5º, inciso VI do MCI, tendo em vista que possibilitam a identificação de outras informações de cunho pessoal, como o nome, conteúdo compartilhado e localização. Tais registros permitem, então, que as plataformas retenham um conjunto de informações, por meio das quais é possível traçar um perfil sobre hábitos, interesses e círculo social dos indivíduos. Trata-se, portanto, daquilo que a literatura especializada tem chamado de "metadados" e que, via de regra, se enquadra na definição de "dado pessoal", na medida em que tornam uma pessoa identificada ou identificável (art. 5º, I, da LGPD) pelo seu comportamento na rede.

A terceira consideração diz respeito à ausência de recomendação expressa para que a neutralidade dos serviços de segurança da informação não seja quebrada. Isso porque, ativar um sistema de armazenamento prévio dos dados que tenha como requisito apenas "o envio em massa", enfraqueceria o mecanismo de criptografia de ponta a ponta (*end-to-end encryption ou E2EE*), que é uma codificação de segurança utilizada pelos aplicativos para assegurar que o conteúdo de uma mensagem só possa ser acessado por quem o envia e quem o recebe. Ou seja, neste modelo, nem mesmo as plataformas têm acesso imediato ao conteúdo das mensagens,

---

[141] STJ, 3ª Turma. RMS nº 62.143/RJ. Rel. Ministro Rogério Schietti Cruz, julgado em 26/08/2020. Disponível em http://www.mprj.mp.br/documents/20184/540394/rms62143.pdf . Acesso em 08 Fev 2021.

cujo sigilo só pode ser "quebrado", em último caso, mediante decisão judicial atendendo a critérios específicos, caso a caso.

Portanto, não é sem fundamento a alegação de que o prévio armazenamento em massa de dados pessoais é medida desproporcional, que confere aos intermediários um amplo conhecimento sobre a vida privada dos usuários, podendo ser entendido como mecanismo de rastreabilidade. Fazendo um breve exercício de comparação, na Ciência da Informação o fator da rastreabilidade está ligado à capacidade de um sistema de descrever o histórico de uma informação, seu percurso e estágio atual, por meio de dados previamente registrados em vários níveis de detalhes, visando compor um banco de informações correlacionais de modo inequívoco (SILVA, 2009, p. 90)[142].

No caso do PL 2630/2020, ao permitir que as plataformas acessem uma quantidade significativa de dados pessoais que, quando associados a outros dados e conteúdos, permitem a identificação de usuários, o fluxo comunicativo e a localização destes, podemos inferir que há brechas legais para a predição de mecanismos de rastreabilidade. Para identificar como essas brechas podem ser lidas na redação atual do artigo 10, sintetizamos, no Quadro 1, os principais problemas, modificações e direitos em jogo na proposta do dispositivo.

A partir das considerações acima, intui-se que se a redação do artigo permite empreender a rastreabilidade como mecanismo de vigilância, forçoso crer que as empresas não a implementariam em benefício de seus modelos de negócio. Afinal, se a lei abre lacunas para que se faça, por que elas não fariam? Ainda mais considerando o princípio de não-afetação da liberdade dos modelos de negócios – que protege a patente algorítmica das *BigTechs* – as vantagens comerciais que poderiam obter com o conhecimento irrestrito dos perfis de consumidores são imensuráveis.

De todo modo, sabemos que argumentos que se baseiam em suposições ou possibilidades fragilizam o debate a respeito das situações concretas que nos circundam. Por outro lado,

[142] SILVA, Claudete A. **Gestão da segurança da informação: um olhar a partir da Ciência da Informação**. Dissertação de Mestrado, Centro de Ciências Sociais Aplicadas, Pós-graduação em Ciência da Informação. Campinas (SP): PUC-Campinas, 2009, p. 90. Disponível em http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui/bitstream/tede/819/1/Claudete%20Aurora%20da%20Silva.pdf. Acesso em 21 Jan 2021.

acreditamos não ser o caso da hipótese verificada neste trabalho, posto que a partir dos embasamentos teóricos e de toda discussão jurídico-legislativa destrinchada até aqui observou-se que as proposições do legislador no PL 2630/2020 têm sido, no mínimo, desatentas aos perigos para os direitos individuais e coletivos envolvidos.

**Quadro 1** - Principais problemas, avanços e direitos abrangidos pela redação do artigo 10 do PL2630/2020

| Texto aprovado | Problemas | Pontos a favor | Direitos em jogo |
|---|---|---|---|
| **Art. 10. Os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses, resguardada a privacidade do conteúdo das mensagens.** | - A identificação e guarda generalizada de dados, sem que haja prévia instauração de inquérito pela autoridade policial ou determinação de autoridade judicial, pode fazer com que pessoas desavisadas, manipuladas ou literalmente desinformadas sejam automaticamente consideradas suspeitas e tenham, por consequência, seus dados pessoais monitorados.<br><br>- Não especifica quais "serviços de mensageria" estão abrangidos por esse dever de armazenamento, deixando brechas para que inclusive os E-mails (que é um tipo de serviço para envio de mensagens) sejam incluídos numa interpretação mais abrangente do artigo.<br><br>- Estabelece procedimentos e prazos não baseados em justificativas técnicas afeta a ingerência das empresas sobre seus sistemas de tratamento de dados e abre caminhos para que elas, por precaução, convencionem medidas de rastreio irrestrito do comportamento humano para se respaldarem. | - Afastou a possibilidade de moderação do conteúdo das mensagens pelas plataformas, previsto na versão original do projeto. | - Risco à **presunção de inocência** e ao **exercício do contraditório.**<br><br>- Relativiza a **proteção dos dados pessoais** enquanto direito fundamental que deve ser lido na regra, e não à exceção.<br><br>- Abuso contra a **liberdade dos modelos de negócios promovidos na internet** (artigo 3º, inciso VIII do MCI). |

**Fonte:** Elaboração da autora, 2021.

| | | | |
|---|---|---|---|
| **§ 1º Considera-se encaminhamento em massa do envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 (quinze) dias, para grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários.** | - Cinco encaminhamentos é um número consideravelmente baixo e pode afetar uma margem considerável de cidadãos comuns desintencionados, considerando a cultura engendrada pelos grupos de *WhatsApp, Telegran* e afins.<br><br>- Não especifica como identificará as mensagens que viralizarão a ponto de, dentro dos 15 dias, ultrapassarem o limite de 1.000 (mil) usuários. Quando será o marco inicial para contar os 15 dias? | - Dificultar a atividade de *bots* ou sistemas automatizados de transmissão. | - Pode afetar a **liberdade de expressão** (artigo 5º, inciso IX da CRFB/88) de pessoas e limitar a **manifestação do pensamento nos meios de comunicação** (artigo 5º, inciso IV e artigo 220, ambos da CRFB/88), sobretudo no caso das pessoas que utilizam os encaminhamentos em massa como um legítimo recurso de engajamento político nos movimentos sociais. |
| **§ 2º Os registros de que trata o *caput* devem conter a indicação dos usuários que realizaram encaminhamentos em massa da mensagem, com data e horário do encaminhamento e o quantitativo total de usuários que receberam a mensagem.** | - A intenção deste parágrafo é atingir apenas as interações de quem disparou as mensagens. Porém, o grande problema está, justamente, em criar critérios para definir qual disparo em massa será considerado suspeito para a guarda de dados e qual não será. Do contrário, considerando a definição de disparo em massa trazida no parágrafo anterior ("uma mesma mensagem transmitida a mais de 5 usuários no intervalo de 15 dias") a maior parte das interações por grupos em aplicativos de mensagem será alvo da guarda de dados, principalmente no cenário eleitoral. | - Tenta delimitar o armazenamento apenas aos dados de quem encaminhou a mensagem, contudo, pelos motivos já expostos, a aplicabilidade dessa determinação continua sendo excessiva e incompatível com o princípio da proteção à privacidade, da proteção dos dados pessoais (artigo 3º, incisos I e II do MCI) e da finalidade e adequação (artigo 6º, incisos I e II da LGPD). | - Pode pôr risco a proteção da **privacidade** e da **intimidade** (artigo 5º, inciso X da CRFB/88) e o **direito à proteção dos dados pessoais** (artigo 3º, incisos I e II do MCI, posteriormente reconhecido como direito fundamental em decisão do STF na ADI 6.387/2020). |

**Fonte:** Elaboração da autora, 2021.

| | | | |
|---|---|---|---|
| **§ 3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento em massa de conteúdo ilícito, para constituição de prova em investigação criminal e em instrução processual penal, mediante ordem judicial, nos termos da Seção IV do Capítulo II da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** | - Os "registros" aos quais se refere o dispositivo são, na verdade, os metadados, assim entendidos pelos serviços de engenharia da informação. Isto é, são os mesmos mencionados no artigo 5º, inciso 6º do MCI. Trata-se de um conjunto de informações referentes "à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados". **Logo, não há como guardar metadados sem identificar previamente, pelo menos, uma cadeia de informações a respeito da data, hora, local e tipo de acesso dos usuários.** Considerando que o *caput* do artigo amplia o espectro de guarda a todos os usuários envolvidos na cadeia de encaminhamento, sem prever critérios e ambientes de armazenamento seguros, mesmo na hipótese de investigação haverá a quebra de sigilo para todo mundo envolvido. | - Tenta harmonizar o dever de guarda com a reserva jurisdicional para o acesso aos dados. Todavia, pelos motivos já expostos, é medida que não se sustenta na prática. A autorização judicial deveria preceder a identificação das mensagens com conteúdo ilícito para tão somente autorizar o armazenamento pelos 15 dias subsequentes. | - A impossibilidade de vedação do acesso ao conjunto de informações gerais que compõem os metadados conduz, por si só, à possibilidade de **violação do sigilo das comunicações** (artigo 5º, inciso XII da CRFB/88). |
| **§ 4º A obrigatoriedade de guarda prevista neste artigo não se aplica às mensagens que alcançarem quantitativo total inferior a 1.000 (mil) usuários, devendo seus registros ser destruídos nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).** | - Mesma hipótese do parágrafo anterior. | - Traz a obrigatoriedade de destruição dos registros como regra e o armazenamento como exceção, tal como prevê o artigo 16 da LGPD, todavia, ainda assim, deixa de especificar que o armazenamento deve ser medida posterior ao tratamento dos dados e para cumprimento de obrigação legal ou regulatória (artigo 16, inciso I da LGPD). | - Mesma hipótese do parágrafo anterior. |

**Fonte:** Elaboração da autora, 2021.

Retomamos, por fim, às considerações de Fernanda Bruno (2009), que nos alerta que os mecanismos de vigilância na sociedade contemporânea nem sempre são coercitivos ou deixam a vista de percepção o seu controle sobre nossas vidas. A propósito, geralmente se mascaram em dispositivos que não são inicialmente projetados para este fim e, como a autora pontua, se distribuem em múltiplas funções sob o manto da legalidade do Estado. Nos parece, portanto, que o artigo 10 do PL 2630/2020 seja um exemplo concreto disso.

# CONCLUSÃO

## É possível combater a desinformação sem infringir a proteção de dados pessoais?

A pergunta que encerra este trabalho traz uma provocação propositiva para o campo dos direitos fundamentais, que têm na Constituição a base principiológica e normativa mais importante para sua garantia e eficácia. Sendo certo que a elasticidade do texto constitucional deve acompanhar às conquistas do passado, olhando para o presente e vislumbrando caminhos futuros, o reconhecimento da autodeterminação informativa e da proteção de dados enquanto direitos fundamentais do nosso tempo é um grande exemplo de que é possível combater a desinformação sem infringir a proteção de dados pessoais.

As discussões oportunizadas até aqui implicam em demonstrar que a desinformação é um problema para a proteção de dados enquanto direito garantido na sua plenitude, e que instituir mecanismos que ofereçam riscos à proteção de dados pessoais para conter esse problema só coloca em desarmonia o dever negativo de intervenção do Estado na vida privada e o dever positivo de proteção às liberdades individuais.

Como visto na seção 1.3, o direito fundamental à proteção de dados abrange um conjunto relativamente flexível de liberdades individuais e bens tutelados, que não precisam "invadir" a seara de proteção uns dos outros; são harmônicos e complementares entre si, e podem ser aplicados em diversos casos envolvendo a coleta, o processamento ou transmissão de dados pessoais. Daí que a necessidade de discutir a finalidade da coleta e armazenamento dos dados pessoais como mecanismo de combate à desinformação se revela mais importante para a avaliação da constitucionalidade das medidas regulatórias do que propriamente a definição de um conceito para o problema.

Todavia, sabemos que a compreensão sobre o que seja a desinformação ainda precisa de amplos debates, conforme enfatizado na primeira seção do Capítulo 1, buscando-se superar o imaginário reduzido às "*Fake News*", de modo que a sociedade seja capaz de identificar suas

causas, efeitos e reflexos para o funcionamento das democracias. Neste sentido, a partir da análise do PL 2630/2020 observamos que se por um lado as discussões legislativas abandonaram o perigo que havia em tentar definir a "desinformação", por outro a proposta que segue em tramitação no Congresso trouxe medidas para coibir a desinformação por meio da moderação dos "comportamentos inautênticos", dando às plataformas o poder de investigação e vigilância das condutas identificadas, por elas, como ilegítimas.

No tocante às medidas específicas do artigo 10, entendeu o legislador que o armazenamento prévio dos dados de todos os usuários envolvidos numa cadeia de encaminhamento em massa, assim definida como "*do envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 (quinze) dias*", evitaria os comportamentos inautênticos e, portanto, a propagação de desinformação.

Ocorre que tal alternativa promove uma disputa complicada para o sopesamento de direitos civis e políticos. Primeiro, porque para que se ampliar o poder de vigilância e apuração de condutas ilícitas, é necessário restringir de algum modo as liberdades individuais. Segundo, porque tornar suspeito o mero encaminhamento em massa para determinar o monitoramento prévio de um usuário ou conta, sem que haja critérios objetivos quanto à intencionalidade da conduta e ao conteúdo (conforme sugerem as teorias da desinformação), invente a lógica da presunção de inocência.

Terceiro, por que por força deste artigo, mobilizações espontâneas de legítima participação política podem expor seus agentes ao rastreamento irrestrito dos intermediários e, ainda, a possíveis violações da privacidade, já que os dados relativos às mensagens (destinatários, local de envio, horário etc) ficarão ao dispor das plataformas. Além disso, a medida desconsidera a dinâmica moral punitiva das redes (como a "militância do cancelamento", por exemplo), que é perigosa e, da forma como ocorre, pode levar as pessoas a se auto incriminarem pelos mecanismos subjetivos de vigilância.

Assim, coloca-se em risco a privacidade e a segurança dos dados pessoais de uma coletividade para atingir comportamentos específicos, cujos desdobramentos tecnológicos certamente dariam conta de burlar esse mecanismo. Além disso, a redação do artigo parece ignorar o funcionamento da estrutura das redes, no qual é praticamente impossível identificar a

autoria e o fim de uma cadeia de encaminhamento de mensagens, levando-se em conta que a convergência midiática permite a replicação de um mesmo conteúdo em vários formatos e redes.

Há, entretanto, alguns pontos do projeto que merecem destaque por terem acolhido boa parte das críticas iniciais, quais sejam: o dever de transparência dos intermediários, com a implementação de relatórios de transparência sobre o processo de remoção e suspensão de contas, conteúdos e disseminadores; e a reserva de jurisdição para o acesso ao conteúdo das mensagens, para constituição de prova em investigação criminal e em instrução processual penal.

Em linhas gerais, a discussão oportunizada neste trabalho, com o amparo das referências teóricas e jurisprudenciais, leva a crer que ampliar medidas de vigilância com o emprego de mecanismos de rastreabilidade é medida excepcional, que só deve ser mobilizada em último caso. Portanto, a guarda, identificação e armazenamento de dados referentes à comunicações em massa sempre devem ser precedidos por ordem judicial, preservando-se o exercício do contraditório e da ampla defesa e obedecendo a critérios específicos para tanto, conforme o debate já empreendido na aprovação do Marco Civil da Internet em 2014.

Anote-se que lá em 2014, diferente do que tem ocorrido na tramitação do PL 2630/2020, o congresso recebeu contribuições de diversos setores da sociedade civil até se chegar ao consenso de que o armazenamento de dados que possam identificar os usuários deveria obedecer ao "princípio da intervenção mínima" e, em último caso, quando determinado por autoridade judicial, poderiam os provedores manter, sob sigilo, em ambiente controlado e de segurança, os dados especificados decorrentes de obrigação (artigos 10 e 13 da Lei 12.965/2014). Ou seja, não todos os dados e tampouco de uma coletividade, sob risco de que o armazenamento prévio configure um mecanismo de "vigilância distribuída" autorizado pela lei.

Por fim, depreende-se que os caminhos para o enfretamento da desinformação passam pela necessidade de que a sociedade e as instituições estejam cientes de como funciona a economia informacional das redes e como seus agentes intermediários elaboram estratégias para capitalizar as informações sobre o comportamento, a vida privada e o pensamento humano.

Daí a importância de se pensar políticas para a promoção da educação midiática, política e científica por um lado e, por outro, para a regulação da sistemática das tecnologias que alimentam o processo de desordem informacional. Mas, ainda que por enquanto a proposta de regulação da desinformação no Brasil esteja em andamento, deixamos aqui a nossa contribuição acadêmica para este debate que, possivelmente, renderá muitos outros capítulos.

# BIBLIOGRAFIA


ABRUSIO et al. **Vigilância em massa ou combate à desinformação: o dilema do rastreamento**. Revista Consultor Jurídico. Coluna Direito Digital. Publicado em 04 Ago 2020. Disponível em https://www.conjur.com.br/2020-ago-04/direito-digital-dilema-rastreamento-pl-fake-news. Acesso em 10 Jan 2021.

ALEMANHA. ***Neztdurchsetzungsgeset - NetzDG***. "Lei de Fiscalização da Rede". Aprovada em 09 Jul 2017. Disponível em https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Acesso em 12 Fev 2021.

BAUMAN, Z.; LYON, D. ***Liquid surveillance: a conversation***. Cambridge: Polity Press, 2013.

BECKER, Howard. **Métodos de pesquisa em ciências sociais**. Tradução: Estevão Renato Aguiar. São Paulo: Editora HUCITEC, 1993, p. 12.

BENJAMIN, Ruha. ***Race after technology: Abolitionist tools for the new Jim Code***. Oxford (UK): Social Forces, 2019.

BENTES, Ivana. **A memética e era da pós-verdade**. Artigo de opinião publicado em 31 Out 2016. Revista Cult, 2016, s.p. Disponível em https://revistacult.uol.com.br/home/a-memetica-e-a-era-da-pos-verdade/. Acesso em 18 Jan 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1ª Edição. Rio de Janeiro: Forense, 2018.

BODIN DE MORAES. **Na medida da Pessoa Humana - Estudos de direito civil-constitucional**. Capítulo II. 1ª Edição. Rio de Janeiro: Editora Renovar, 2010, p. 121-148. Disponível em https://www.researchgate.net/publication/288490662_Ampliando_os_direitos_da_personalidade . Acesso em 18 Jan 2021.

BRASIL. **Constituição da República Federativa de Brasil**, de 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 28 Jan 2021.

_____. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei 13.709, de 14 de agosto de 2018. Brasília, DF: Diário Oficial da União, 15 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm . Acesso em 28 Jan 2021.

_____. **Marco Civil da Internet**. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Diário Oficial da União, 24 de abril de 2014. Disponível em http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm . Acesso em 28 Jan 2021.

BRUNO, Fernanda. Mapas de crime: vigilância distribuída e participação na Cibercultura. **Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação**. E-Compós, v.12, n.2. Brasília: maio/ago, 2009, p. 1-16. Disponível em http://www.e-compos.org.br/e-compos/article/download/409/352. Acesso em 15 Jan 2021.

_____. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade.** Porto Alegre, Sulina, 2013.

BUONANNO, Milly. Uma eulogia (prematura) do broadcast: o sentido do fim da televisão. **Revista Matrizes** (USP). v. 9, nº 1, Jan-Jun de 2015. São Paulo: USP, 2015, p. 67-86. Disponível em https://core.ac.uk/download/pdf/268325468.pdf. Acesso em 22 Jan 2021.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional. **Revista de Direito do Consumidor**, v. 46, Edição Abril a Junho. São Paulo, 2003, p. 77-119.

CASTELLS, Manuel. **A sociedade em rede. A era da informação: economia, sociedade e cultura**. Vol. 1. 2ª Edição. São Paulo: Paz e Terra, 1999, p. 565.

CDA. "***Communications Decency Act***" (1996). Disponível em https://www.law.cornell.edu/uscode/text/47/230 . Acesso em 12 Fev 2021.

DARNTON, Robert. **A verdadeira história das notícias falsas: séculos antes das redes sociais, os boatos e as mentiras alimentavam pasquins e gazetas na Europa**. El País Brasil, publicado em 1 mai 2017. Disponível em https://brasil.elpais.com/brasil/2017/04/28/cultura/1493389536_863123.html. Acesso em 12 Jan 2021.

DATA PRIVACY BRASIL. Rastreabilidade, metadados e Direitos Fundamentais: nota técnica sobre o projeto de Lei 2630/2020. Disponível em https://www.dataprivacybr.org/wp-content/uploads/2020/07/Data-Privacy-Brasil.-Rastreabilidade-e-Direitos-Fundamentais.-PL-2630.2020.pdf. Acesso em 27 Jan 2021.

DE PAULA, Felipe; PAIVA, Luiz Guilherme M de. **A pesquisa legislativa: fontes, cautelas e alternativas à abordagem tradicional**. In: QUEIROZ, Rafael Maffei R.; FEFERBAUM, Marina (Coord.). Metodologia da pesquisa em direito: técnicas e elaboração de monografias, dissertações e teses. 2ª Edição. São Paulo : Saraiva, 2019, p. 138-163.

DELEUZE, Gilles. **Conversações**. Rio de Janeiro: Editora 34, 1992, p. 220-227.

DMCA. "***Digital Millennium Copyright Act***" (1998). Disponível em https://www.copyright.gov/legislation/dmca.pdf. Acesso em 12 Fev 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1ª Edição. Rio de Janeiro: Renovar, 2006.

EUA. **Princípios de Santa Clara sobre Transparência e Accountability em Moderação de Conteúdo**. Publicado em 7 Mai 2018. Disponível em https://santaclaraprinciples.org/. Acesso em 12 Fev 2021.

FALLIS, Don. *What Is Disinformation?*. In: HEROLD, Ken (Coord.). *Exploring Philosophies of Information*. ***Library Trends***, Vol. 63, nº3. University of Illinois, 2015, p. 401-426. Disponível em https://www.ideals.illinois.edu/bitstream/handle/2142/89818/63.3.fallis.pdf?sequence=2. Acesso em 12 Jan 2021.

FILIPINAS. **Princípios de Manila sobre Responsabilização de Intermediários**. Publicado em 30 Mai 2015. Disponível em https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf. Acesso em 12 Fev 2021.

FOUCAULT, Michel. **Em defesa da sociedade**. Tradução: Maria Ermantina Galvão. São Paulo: Martins Fontes, 2002, p. 289.

_____. **Vigiar e punir: nascimento da prisão**. Tradução: Raquel Ramalhete. 42ª Edição. Petrópolis: Editora Vozes, 2014, p. 194-202.

FRAGA, Alex Branco. **Exercício da informação: governo dos corpos no mercado da vida ativa**. Campinas: Autores Associados, 2006, 185 p.

HLEG. "***A multi-dimensional approach to disinformation***"**.** Report of the independent High level Group on *Fake News* and online disinformation". Luxembourg: Publications Office of the

European Union, 2018, p.3. Disponível em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271 . Acesso em 12 Jan 2021.
LEMOS, Ronaldo; Carlos Affonso SOUZA. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016,P. 16-17. Disponível em https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em 15 Jan 2021.
LIMBERGER, Têmis. A informática e a proteção à intimidade. **Revista de Direito Constitucional e Internacional**. v. 8, n. 33, Edição de Outubro a Dezembro. São Paulo: Revista dos Tribunais, 2000, p. 110–124.
LYON, David. A cultura da vigilância: envolvimento, exposição e ética na modernidade digital. In: BRUNO, Fernanda *et al* (Org.). **Tecnopolíticas da vigilância: perspectivas da margem**. Tradução: Heloísa Cardoso Mourão et al.1ª Edição. São Paulo: Editora Boitempo, 2018 [2017], p.151-180.
MARCHAL, N., KOLLANYI, B., NEUDERT, L. M., & HOWARD, P. N. *Junk news during the EU parliamentary elections: Lessons from a seven-language study of Twitter and Facebook. **Online Supplement to Data Memo***, May 2019. Oxford Internet Institute, 2019, 1-12. Disponível em https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/EU-Parliamentary-Elections-Supplement.pdf. Acesso em 12 Jan 2021.
ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em 12 Jan 2021.
ORWELL, George. **1984**. São Paulo: IBEP, 2003.
QUEIROZ, Rafael Mafei R. **Metodologia da pesquisa jurídica**. In: CAMPILONGO, Celso F,; GONZAGA, Alvaro de A.; FREIRE, André Luiz(coords.). Enciclopédia jurídica da PUC-SP. 1ª Edição. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em https://enciclopediajuridica.pucsp.br/verbete/151/edicao-1/metodologia-da-pesquisa-juridica. Acesso em 12 Fev 2021.
RIBEIRO, Luciana Antonini. A privacidade e os arquivos de consumo na Internet: uma primeira reflexão. **Revista do Direito do Consumidor**. V. 11, nº 41, Edição Janeiro a Março. São Paulo, 2002,p. 151-165.
RODOTÀ, Stefano. **A vida na sociedade de vigilância. Privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 36-45.
RODRIGUEZ, Pablo E. Espetáculo do dividual: tecnologias do eu e vigilância distribuída nas redes sociais. Tradução de María Sandra Arencón Beltrán e Marta Mourão Kanashiro. In: BRUNO, Fernanda *et al* (Org.). **Tecnopolíticas da vigilância: perspectivas da margem**. 1ª Edição. São Paulo: Editora Boitempo, 2018 [2015], p.182-198.
SAMPAIO, José Adércio L. **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais**. Belo Horizonte: Del Rey, 1998, p.262-264.
SARLET, Ingo W. **A eficácia dos direitos fundamentais**. 2ª. Ed. Porto Alegre: Livraria do Advogado, 2001. p. 97-102.
SCHERTEL MENDES, L. et al (Orgs.). **Tratado de proteção de dados pessoais**. (E-book não-paginado). Parte 1 - Fundamentos teóricos e históricos da proteção de dados pessoais. 1ª Edição. Rio de Janeiro: Editora Forense, 2020, sem paginação.
SENADO FEDERAL. **PL nº 2630/2020**. Proposta original protocolada em 13 Mai 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8110634&ts=1612303001672&disposition=inline. Acesso em 10 Dez 2020.

SENADO FEDERAL. **PL nº 2630/2020**. Texto substitutivo aprovado em 30 Jun 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8128670&ts=1612303015028&disposition=inline. Acesso em 10 Dez 2020.

SIBÍLIA, Paula. **O show do eu: a intimidade como espetáculo**. 2ª Edição. Rio de Janeiro: Contraponto, 2016, p.55-124.

SILVA, Claudete A. **Gestão da segurança da informação: um olhar a partir da Ciência da Informação**. Dissertação de Mestrado, Centro de Ciências Sociais Aplicadas, Pós-graduação em Ciência da Informação. Campinas (SP): PUC-Campinas, 2009, p. 90. Disponível em http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui/bitstream/tede/819/1/Claudete%20Aurora%20da%20Silva.pdf. Acesso em 21 Jan 2021.

SOUZA, Rebeca H. V. de; SOLAGNA, Fabrício; LEAL, Ondina F. As políticas globais de governança e regulamentação da privacidade na internet. **Revista Horizonte Antropológico**, v. 20, n. 41, Junho de 2014. Porto Alegre: IFCH-UFRGS, 2014, p. 141-172. Disponível em https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-71832014000100006. Acesso em 12 Fev 2021.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento Civil-constitucional brasileiro. In:____. **Temas de direito civil. Rio de Janeiro**: 2001, p. 23-54.

UE. **Código de condutas sobre Desinformação**. Publicado em Abr 2018 Disponível em https://ec.europa.eu/digital-single-market/en/code-practice-disinformation. Acesso em 12 Fev 2021.

UE. **Diretiva 2016/0280**, de 15 Abr 2019. Disponível em https://data.consilium.europa.eu/doc/document/PE-51-2019-INIT/en/pdf. Acesso 12 Fev 2021.

VIANA, Tulio. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003, p. 13-26.

VOLKOFF, Vladimir. **Pequena história da desinformação: do cavalo de Tróia à Internet**. Curitiba: Editora Vila do Príncipe, 2004, p. 32-33.

WALDMAN, Ari Ezra. *The Marketplace of Fake News*. Vol. 20. **University of Pennsylvania Journal of Constitutional Law**, 2017, p. 845-870. Disponível em https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1661&context=jcl. Acesso em 12 Jan 2021.

WARDLE, Claire; DERAKHSHAN, Hossein. *Information Disorder: Toward an interdiciplinary framewok for research and policy making*. **Council of Europe report (DGI)**, 2017, p. 20-26. Disponível em https://www.researchgate.net/publication/339031969_INFORMATION_DISORDER_Toward_an_interdisciplinary_framework_for_research_and_policy_making_Information_Disorder_Toward_an_interdisciplinary_framework_for_research_and_policymaking. Acesso em 27 Dez 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v.4, n.5. BOSTON, US: 1890, sem paginação. Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em 12 Jan 2021.

ZANATTA, Rafael A. F. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. In: ABRAMOVAY, Ricardo; ZANATTA, Rafael A. F. Risk regulation and data protection. (research project). Brasil: Researchgate, 2019, p. 3. Disponível em https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos

_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais. Acesso 27 Jan 2021

ZUBOFF, 2019 *apud* KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. **Revista Brasileira de Ciências Sociais.** V. 36, nº. 105, e3610514. São Paulo: ANPOCS, 2021, p.1-6. Disponível em https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-69092021000100702&lng=en&nrm=iso&tlng=pt. Acesso em 23 Jan 2021.

ZUBOFF, Shoshana. *Big Other: surveillance capitalism and the prospects of an information civilization*. **Journal of Information Technology**. V. 30, nº1. US: Sage Publishing, 2015. Disponível em https://journals.sagepub.com/doi/10.1057/jit.2015.5. Acesso em 18 Dez 2020.

ZUBOFF, Shoshana. ***The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power***. New York: PublicAffairs, 2019.